Zmluva o dielo č. 645/2025/OIT

„Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica"

uzatvorená v zmysle § 536 a nasl. zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších zmien a doplnkov

(ďalej v texte len „Zmluva")

Zmluvné strany:

Objednávateľ:	Mesto Banská Bystrica
Sídlo:	Československej armády 26, 974 01 Banská Bystrica
V mene ktorého koná :	MUDr. Ján Nosko, primátor mesta
Osoba oprávnená na rokovanie	
vo veciach zmluvných:	Ing. Alexander Hlavatý, email: alexander.hlavaty@banskabystrica.sk tel.: 048/ 4330 330
vo veciach NFP:	Ing. Beáta Galková, email: beata.galkova@banskabystrica.sk tel.: 048 / 4330 442
vo veciach technických:	Ing. Alexander Hlavatý, email: alexander.hlavaty@banskabystrica.sk
(technický dozor)	tel.: 048/ 4330 330 Ing. Bibiána Palušková, e-mail: bibiana.paluskova@banskabystrica.sk tel.: 048 / 4330 336,
Bankové spojenie:	Československá obchodná banka, a. s., pobočka Banská Bystrica
BIC:	CEKOSKBX
IBAN:	SK73 7500 0000 0040 1714 6450
IČO:	00 313 271
DIČ:	2020451587
IČ DPH:	SK2020451587

(ďalej v texte len „**Objednávateľ**")

Zhotoviteľ:	Slovanet, a.s.
Sídlo:	Galvaniho 19, 821 04 Bratislava
Zápis v OR:	OR Mestského súdu Bratislava III, Oddiel: Sa, vložka č.: 3692/B
V mene ktorého koná :	Ing. Peter Máčaj, predseda predstavenstva
Osoby oprávnené na rokovanie:	
vo veciach zmluvných:	RNDr. Lukáš Karlík, PhD., tel.:
vo veciach technických:	Ing. Peter Ličko,
tel. kontakt:	
Bankové spojenie:	
BIC:	
IBAN:	
IČO:	35 954 612
DIČ:	2022059094
IČ DPH:	SK2022059094

(ďalej v texte len „**Zhotoviteľ**")

(ďalej v texte spolu aj len „**Zmluvné strany**")

Úvodné ustanovenia

Predmetná zmluva je výsledkom verejnej súťaže, vyhlásenej Objednávateľom ako verejným obstarávateľom v súlade so zákonom č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej v texte len **„zákon o verejnom obstarávaní"**) na obstaranie zákazky: **„Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica"**.

Článok I.
PREDMET ZMLUVY

1. Predmetom tejto zmluvy je záväzok Zhotoviteľa riadne a včas, na svoje náklady a vlastné nebezpečenstvo, v rozsahu a za podmienok bližšie špecifikovaných podkladovou dokumentáciou v zmysle bodu 2. tohto článku Zmluvy a za podmienok stanovených v tejto Zmluve, zrealizovať pre Objednávateľa dielo: **„Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica"** (ďalej v texte len **„Dielo"**), ktoré pozostáva z nasledovných častí:
   a) Vypracovanie relevantnej bezpečnostnej dokumentácie;
   b) Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica;
   c) Vykonanie segmentácie siete Mesta Banská Bystrica s ohľadom na súčasné prevádzkové požiadavky;
   d) Zrealizovanie výmeny aktívnych prvkov core časti siete;
   e) Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete;
   f) Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

   (ďalej v texte len **„Časti diela"**).

2. Podkladovú dokumentáciu pre Dielo tvoria nasledovné dokumenty:
   - Projektový zámer,
   - Prístup k projektu,
   - Funkčná špecifikácia,
   - Žiadosť o nenávratný finančný príspevok (ďalej v texte len **„ŽoNFP"**),
   - Súťažné podklady vrátane ich príloh,
   - Vysvetlenia súťažných podkladov a súvisiacich dokumentov (ak k vysvetľovaniu v procese verejného obstarávania došlo),
   - Ponuka Zhotoviteľa ako úspešného uchádzača predložená v procese verejného obstarávania vrátane jej príloh,

   (ďalej v texte len **„Podkladová dokumentácia"**). Projektový zámer, prístup k projektu a funkčná špecifikácia tvoria prílohu č. 1 tejto Zmluvy.

3. Zhotoviteľ sa zaväzuje pre jednotlivé Časti diela zhotoviť a odovzdať Objednávateľovi Dielo v rozsahu Podkladovej dokumentácie nasledovne :
   3.1. Komplexné služby pri vypracovaní relevantnej bezpečnostnej dokumentácie a zosúladení so zákonnými požiadavkami kladenými na poskytovateľa základnej služby v etapách:
      3.1.1. Analýzy a dizajn
      3.1.2. Implementácia
      3.1.3. Nasadenie a postimplementačná podpora
   3.2. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta v etapách:
      3.2.1. Analýzy a dizajn
      3.2.2. Nákup technických prostriedkov, programových prostriedkov a služieb
      3.2.3. Implementácia a testovanie
      3.2.4. Nasadenie a postimplementačná podpora
   3.3. Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky v etapách:
      3.3.1. Analýzy a dizajn
      3.3.2. Implementácia a testovanie
      3.3.3. Nasadenie a postimplementačná podpora
   3.4. Výmena aktívnych prvkov CORE časti siete v etapách:
      3.4.1. Analýzy a dizajn
      3.4.2. Nákup technických prostriedkov, programových prostriedkov a služieb
      3.4.3. Implementácia a testovanie
      3.4.4. Nasadenie a postimplementačná podpora
   3.5. Implementácia systému dvojfaktorovej autentifikácie v etapách:
      3.5.1. Analýzy a dizajn

3.5.2. Nákup technických prostriedkov, programových prostriedkov a služieb
3.5.3. Implementácia a testovanie
3.5.4. Nasadenie a postimplementačná podpora

3.6. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice v etapách:
3.6.1. Analýzy a dizajn
3.6.2. Nákup technických prostriedkov, programových prostriedkov a služieb
3.6.3. Implementácia a testovanie
3.6.4. Nasadenie a postimplementačná podpora

(ďalej v texte len **„Predmet plnenia“).**

4. Záväzku Zhotoviteľa podľa bodu 1. tohto článku Zmluvy zodpovedá záväzok Objednávateľa Dielo zhotovené včas, v rozsahu a za podmienok stanovených v tejto Zmluve prevziať a zaplatiť Zhotoviteľovi cenu za dielo bližšie špecifikovanú v článku V. tejto Zmluvy.

5. Vecné vymedzenie Predmetu plnenia a rozsahu plnenia podľa tejto Zmluvy je špecifikované v článku II. Zmluvy.

6. Zhotoviteľ deklaruje, že sa v plnom rozsahu oboznámil s rozsahom a povahou Predmetu plnenia podľa tejto Zmluvy, že sú mu známe technické, technologické a kvalitatívne podmienky potrebné na realizáciu Diela a že disponuje takými kapacitami a odbornými znalosťami, ktoré sú na plnenie predmetu Zmluvy potrebné.

Článok II.
VECNÉ VYMEDZENIE PREDMETU PLNENIA

1. Zhotoviteľ v zmysle článku I. bod 1. tejto Zmluvy preberá na seba záväzok realizovať Dielo a odovzdať ho Objednávateľovi v rozsahu:

1.1. v Časti diela podľa článku I. bod 1. písm. a) Zmluvy nasledovne:

- Poskytnutie komplexných služieb pri vypracovaní relevantnej bezpečnostnej dokumentácie a zosúladení so zákonnými požiadavkami kladenými na poskytovateľa základnej služby:
- Vykonanie inventarizácie aktív vrátane klasifikácie informácií a kategorizácie sietí a informačných systémov;
- Vypracovanie analýzy rizík podľa požiadaviek uvedených v zákone č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej v texte len **„zákon o kybernetickej bezpečnosti“**) ;
- Vypracovanie analýzy dopadov a kľúčových procesov a činností (ďalej v texte len „BIA“) vrátane prípravy smernice/metodiky pre riadenie kontinuity činností (ďalej v texte len „BCM“), prípravy plánov BCM a plánov obnovy (ďalej v texte len „DRP“).
- Vypracovanie základných bezpečnostných politík podľa zákona o kybernetickej bezpečnosti:
  - Bezpečnostná stratégia kybernetickej bezpečnosti;
  - Politika organizácie bezpečnosti;
  - Politika pre riadenie bezpečnosti rizík;
  - Politika pre riadenie informačných aktív;
  - Pravidlá správania a dobrej praxe;
  - Politika pre riadenie dodávateľských vzťahov;
  - Politika pre riadenie vývoja a údržby v oblasti informačno-komunikačných technológií (ďlaej v texte len „IKT“);
  - Politika pre riadenie a prevádzku IKT;
  - Politika pre riadenie súladu;
  - Politika pre riadenie kontinuity procesov a činností;

1.2. v Časti diela podľa článku I. bod 1. písm. b) Zmluvy nasledovne:

- Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica: obstarať a nasadiť softvérové (ďalej v texte len „SW“) riešenie, pomocou ktorého bude možné vykonávať centralizovanú autentifikáciu a autorizáciu pre rôzne typy používateľov a zariadení v sieti, spravovať politiky prístupu na základe definovania identít, rolí,

zariadení, prípadne ďalších správcom siete voliteľných atribútov, sledovať a revidovať prístupy používateľov do siete, spravovať prístupy do siete zariadeniami pristupujúcimi v režime BYOD („Bring Your Own Device") – zariadení, ktoré nie sú v správe a priamej kontrole správcu IKT Mesta. Nasadené riešenie musí podporovať štandard IEEE 802.1X pre autentifikáciu a autorizáciu zariadení, ktoré budú nadväzovať spojenie so sieťou Mesta. Riešenie musí zabezpečovať kontrolu prístupu do siete na úrovni portov na aktívnych sieťových prvkoch. Pre účely plnohodnotného nasadenia overovania na úrovni celej siete organizácie je potrebné realizovať výmenu sieťových prvkov, ktoré sú „end-of-sales" a „end-of-support" a súčasne nepodporujú protokol 802.1X. v celkovom počte 7 ks;

1.3. v Časti diela podľa článku I. bod 1. písm. c) Zmluvy nasledovne:

- Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky: poskytnúť služby činností expertov na sieťové a bezpečnostné technológie, ktorí vykonajú analýzu súčasného stavu, navrhnú optimálny budúci stav a zaistia vykonanie samotnej segmentácie siete v kontexte implementovaného overovania podľa 802.1X a obstaraných ako aj jestvujúcich aktívnych prvkov siete;

1.4. v Časti diela podľa článku I. bod 1. písm. d) Zmluvy nasledovne:

- Výmena aktívnych prvkov CORE časti siete: obstaranie a dodanie 9 ks aktívnych prvkov pre CORE časť siete súčasne s vykonaním revízie konfigurácie a implementácie nových konfiguračných pravidiel vrátane pravidiel na firewalloch aktívnych prvkov pre CORE časť siete, ktoré budú funkčne a výkonnostne zodpovedať požiadavkám na „TO-BE" stav nie len s ohľadom na celkový performance siete, ale aj s ohľadom na vysoké štandardy bezpečnosti siete;

1.5. v Časti diela podľa článku I. bod 1. písm. e) Zmluvy nasledovne:

- Implementácia systému dvojfaktorovej autentifikácie: obstaranie, analýza, nasadenie a konfigurácia riešenia dvojfaktorovej autentifikácie s celkovým počtom softvérových a hardvérovýych (ďalej v texte len „HW") tokenov pre 700 používateľov. Riešenie musí byť realizované prostredníctvom HW/SW tokenu, ktorý bude generovať jednorazové heslá (OTP – One Time Passwords) pre používateľov prihlasujúcich sa do siete. Používateľ získa OTP prostredníctvom HW zariadenia a SW tokenu nainštalovaného na koncovej stanici. Riadenie identít dvojfaktorového overenia sa bude realizovať prostredníctvom platformy nasadenej na infraštruktúre dodávateľa, ktorý zabezpečí s ohľadom na konkrétnu implementáciu nevyhnutné výpočtové zdroje. Súčasťou dodávky musí byť integrácia dvojfaktorového overovania na jestvujúci systém pre správu identity.

1.6. v Časti diela podľa článku I. bod 1.1. f) tejto zmluvy nasledovne:

- Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice: dodanie systému centrálneho dohľadu a manažmentu koncových zariadení pre minimálne 700 koncových staníc s detekciou nevyžiadanej aktivity, funkcionalitou monitoringu prevádzky na koncovom zariadení a funkcionalitou možnosti centrálneho nastavovania bezpečnostných pravidiel na koncových staniciach. Vykonanie úvodnej analýzy, konfigurácie a nasadenie v produkčnom prostredí.

2. Zhotoviteľ sa za účelom využitia Diela v praxi počas výkonu bežnej agendy Objednávateľa zaväzuje poskytnúť Objednávateľovi školenia k jednotlivým Častiam diela. Osoby, ktorým má byť školenie poskytnuté určí Objednávateľ.

3. Zhotoviteľ sa zaväzuje vypracovať a odovzdať Objednávateľovi relevantnú bezpečnostnú dokumentáciu a komplexnú technickú a používateľskú dokumentáciu v zmysle platnej legislatívy pre informačné technológie verejnej správy (ďalej v texte len „ITVS"). Zhotoviteľ zabezpečí nevyhnutný rozsah dokumentácie v zmysle Vyhlášky č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v rozsahu minimálnych požiadaviek na dokumentáciu a výstupy relevantné pre školenia. Dokumentáciu Zhotoviteľ poskytne v slovenskom jazyku v elektronickej forme na digitálnych médiách (USB kľúč) v počte 3ks v editovateľnej podobe (.docx) a v tlačovej podobe (.pdf). Akékoľvek zmeny v dokumentácii (pridanie nových funkcií, opráv, zmien) budú tieto vždy bez zbytočného odkladu poskytnuté Zhotoviteľom v elektronickej verzii dokumentácie, počas trvania služby podpory.

4. Pred odovzdaním Diela ako celku sa Zhotoviteľ zaväzuje nasadiť Dielo do testovacej prevádzky systémového riešenia, a to v celom rozsahu Predmetu plnenia podľa článku I. bod 3.1. až 3.6. Zmluvy (ďalej v texte len **„testovacia prevádzka"**), pričom:

4.1. Zhotoviteľ sa zaväzuje nasadiť dielo do testovacej prevádzky v lehote do 8 mesiacov odo dňa účinnosti tejto Zmluvy;

4.2. Nasadením do testovacej prevádzky sa zahájí akceptačný proces. Dĺžka trvania akceptačného procesu je po dobu trvania najviac tridsať (30) kalendárnych dní, pričom lehota na zhotovenie Diela ako celku, podľa článku III. Zmluvy musí zostať zachovaná. Objednávateľ sa zaväzuje zabezpečiť všetku nevyhnutnú súčinnosť tak, aby bola testovacia prevádzka a akceptačný proces úspešne ukončený v uvedenej lehote. Ak podmienky poskytnutia nevyhnutnej súčinnosti nie sú výslovne uvedené v Zmluve alebo poskytnutie nevyhnutnej súčinnosti nevyplýva z povahy takejto súčinnosti, je Zhotoviteľ povinný na poskytnutie nevyhnutnej súčinnosti vyzvať Objednávateľa a poskytnúť mu primeranú lehotu na poskytnutie nevyhnutnej súčinnosti. Zhotoviteľ nebude v omeškaní s plnením svojich záväzkov, ak takýto záväzok nemôže riadne a včas splniť pre neposkytnutie nevyhnutnej súčinnosti zo strany Objednávateľa. Akceptačný proces zahŕňa overenie dodaného Diela porovnaním jeho skutočných vlastností s ich špecifikáciou stanovenou v Podkladovej dokumentácii. Akceptačný proces zahŕňa akceptačné testy, ktoré budú prebiehať na základe špecifikácie akceptačných testov vypracovaných a odsúhlasených Zhotoviteľom. Zhotoviteľ je povinný poskytnúť návrh špecifikácie akceptačných testov, vrátane testovacích scenárov, najneskôr do päť (5) pracovných dní pred dohodnutým dňom nasadenia Diela do testovacej prevádzky, resp. začatím nového/opakovaného akceptačného testovania po zapracovaní opráv. Zhotoviteľ má právo vyjadrovať sa a požadovať zapracovanie svojich odôvodnených pripomienok k špecifikácii akceptačných testov a ďalším parametrom akceptačného testovania (akceptačné scenáre a pod.). Zhotoviteľ je povinný všetky požiadavky Objednávateľa splniť bez zbytočného odkladu a predložiť neodkladne plnenie k čiastkovému opakovanému akceptačnému testovaniu. Akceptačný proces sa bude opakovať, kým príslušné zapracovanie pripomienok Objednávateľa nesplní požadované akceptačné kritériá.

4.3. Zhotoviteľ počas testovacej prevádzky garantuje najmä:

- priamy kontakt na pracovníka (Single Point of Contact / ďalej len „SPOC"/) v pracovnej dobe za účelom nahlasovania a riešenia vád zistených počas testovacej prevádzky a/alebo akceptačného testovania,
- reakčnú dobu pre všetky kategórie vád zistených počas testovacej prevádzky a/alebo akceptačného testovania max. dve (2) hodiny od nahlásenia SPOC,
- dobu vyriešenia kritických vád (výpadok celého systému, nedochádza k logovaniu udalostí zo žiadneho zdroja, výpadok dlhší ako tridsať (30) minút) zistených počas testovacej prevádzky a/alebo akceptačného testovania max. dvadsaťštyri (24) hodín od nahlásenia SPOC,
- dobu vyriešenia iných ako kritických vád (výpadok čiastkového komponentu, ktorý nemá vplyv na funkčnosť systému ako celku) zistených počas testovacej prevádzky a/alebo akceptačného testovania max. sedemdesiatdva (72) hodín od nahlásenia SPOC,
- dostupnosť potrebného počtu pracovníkov v pracovnej dobe (v pohotovosti) pre zásahy súvisiace s odstránením vád zistených počas akceptačného testovania. Pracovnou dobou sa pre účely tejto zmluvy rozumejú pracovné dni od 9:00 do 17:00,
- nepretržité riešenie vád v poradí podľa dohody medzi SPOC a zástupcom Objednávateľa,
- pravidelné pracovné stretnutia medzi zástupcami Zhotoviteľa a Objednávateľa, minimálne raz týždenne.

4.4. Ak nebude v rámci testovacej prevádzky preukázaná plná funkčnosť Diela a/alebo odstránené všetky vady zistené počas akceptačného testovania, resp. z dôvodov neposkytnutia nevyhnutnej súčinnosti zo strany Zhotoviteľa, môže byť lehota na ukončenie akceptačného procesu výnimočne

predĺžená o ďalších max. desať (10) kalendárnych dní, pričom lehota na zhotovenie Diela ako celku, podľa článku III. Zmluvy, musí zostať zachovaná.

5. Zhotoviteľ sa zaväzuje poskytnúť Objednávateľovi zaškolenie a postimplementačnú podporu, pričom:
   5.1. Súčasťou Predmetu plnenia je zaškolenie používateľov/administrátorov informačných systémov, pre zabezpečenie administrácie funkcionality v rámci daného riešenia. Zaškolenie bude minimálne v rozsahu 3 x 8 hodín pre 3 – 6 zamestnancov Objednávateľa a bude vykonané v slovenskom jazyku, v priestoroch určených Objednávateľom;

   5.2. Zhotoviteľ zabezpečí, formou konzultačných hodín, odbornú technickú podporu pre dodané riešenie v rozsahu dvoch (2) hodín mesačne. Odborná technická pomoc sa použije na poskytovanie pokročilej technickej asistencie pri plánovaných zmenách v prevádzkových nastaveniach a funkčnosti riešenia a technická asistencia vo forme projekčných postupov pre plánované upgrady, na základe požiadavky Objednávateľa;

   5.3. Postimplementačnú podporu (technickú podporu a servis prevádzkovaných informačných technológií) poskytne Zhotoviteľ počas trvania záručnej doby bližšie špecifikovanej v článku VII. bod 3. Zmluvy.

6. S prihliadnutím na skutočnosť, že všetky IT systémy prechádzajú kontinuálnym vývojom, Zhotoviteľ sa zaväzuje, že nasadenie Predmetu plnenia bude mať možnosť kontinuálnych upgradov, aktualizácií, doplňovania a rozširovania jeho možností minimálne počas trvania záručnej doby bližšie špecifikovanej v článku VII. bod 3. Zmluvy. Kontinuálne upgrady, aktualizácie, doplňovania a rozširovania možností Diela sú zahrnuté v cene za Dielo podľa článku III. Zmluvy.

7. Zhotoviteľ sa zaväzuje, že Predmet plnenia bude zahŕňať dodávku kompletných licencií na používanie SW riešení implementovaných do informačných systémov tvoriacich súčasť Diela, vrátane licenčného maintenance v trvaní minimálne počas trvania záručnej doby bližšie špecifikovanej v článku VII. bod 3. Zmluvy, pričom:
   7.1. Dodaný Predmet plnenia musí zahŕňať implementačné a servisné služby pre danú technológiu, minimálne v rozsahu:
      a) technické inštalácie a implementácie všetkých SW, ktoré budú súčasťou riešenia,
      b) napojenie a integrácia do aktuálneho prostredia Objednávateľa;

   7.2. Licenčný maintenance musí zahŕňať minimálne:
      a) poskytnutie záruky/záručnej aplikačnej podpory na SW komponenty, v trvaní podľa výrobcom stanovenej záručnej doby,
      b) nárok na inštaláciu nových verzií jednotlivých SW počas obdobia, pre ktoré je zaplatená podpora SW komponentov, a to v súlade s licenčnými podmienkami výrobcu SW,
      c) prístup k správam o úpravách a údržbe (patches) SW komponentov, a to v súlade s licenčnými podmienkami výrobcu SW;

   7.3. Zhotoviteľ vyhlasuje, že práva Objednávateľa k Dielu, nadobudnuté na základe licencie, budú bez akýchkoľvek právnych vád a používaním licencie v súlade s touto Zmluvou nedôjde zo strany Objednávateľa k porušeniu právnych predpisov a/alebo k neoprávnenému zásahu do práv tretích osôb;

   7.4. Ak Zhotoviteľ uskutočnením Diela alebo jeho realizáciou, prípadne realizáciou jeho časti, ktorá bude predstavovať autorské dielo, poveril tretiu osobu, je Zhotoviteľ povinný zabezpečiť, aby mu táto osoba udelila licenciu a/alebo sublicenciu na jeho použitie v rozsahu rovnakom ako je uvedené v tomto článku Zmluvy tak, aby licenciu (sublicenciu) bol oprávnený udeliť Objednávateľovi a/alebo previesť ju na Objednávateľa v súlade s touto Zmluvou.

7.5. Pre prípad, že vyhlásenia Poskytovateľa podľa tohto článku Zmluvy sa ukážu byť nepravdivými, Zhotoviteľ sa zaväzuje nahradiť Objednávateľovi všetku škodu, ktorá mu v dôsledku nepravdivých vyhlásení Zhotoviteľa vznikne;

7.6. Zhotoviteľ sa zaväzuje poskytnúť Objednávateľovi všetku potrebnú súčinnosť, v súvislosti s uplatňovaním a/alebo bránením užívateľských práv Objednávateľa k SW riešeniam, implementovaným do informačných systémov tvoriacich súčasť Diela.

7.7. V prípade, že počas platnosti a účinnosti tejto zmluvy alebo po jej skončení, sa zistí akékoľvek porušenie práv duševného vlastníctva tretích osôb v dôsledku konania Zhotoviteľa, Zhotoviteľ sa zaväzuje, že na vlastné náklady usporiada takéto práva a uspokojí nároky tretích osôb v plnom rozsahu;

7.8. Zmluvné strany sa výslovne dohodli, že cena za poskytnutie všetkých licencií potrebných na zabezpečenie realizácie a následnej funkčnosti a prevádzkyschopnosti Diela je zahrnutá v cene za Dielo bližšie špecifikovanej v článku V. bod 2. Zmluvy.

8. Zhotoviteľ sa zaväzuje poskytnúť k dodanému predmetu plnenia záručnú aplikačnú podporu (ďalej v texte len „ZAP“) v trvaní minimálne počas trvania záručnej doby bližšie špecifikovanej v článku VII. bod 3. Zmluvy, pričom:
   8.1. Zhotoviteľ sa zaväzuje poskytnúť k dodanému predmetu plnenia štandardnú prevádzkovú podporu a údržbu (ďalej v texte len „SLA“) v trvaní minimálne počas trvania záručnej doby bližšie špecifikovanej v článku VII. bod 3. Zmluvy;
   8.2. Služby štandardnej prevádzkovej podpory a záručnej aplikačnej podpory pri dostupnosti 5x10 (7:00-17:00) zahŕňajú:
      a) Hotline (neobmedzený počet nahlasovateľov vád zo strany Objednávateľa), resp. priamy kontakt na pracovníka (Single Point Of Contact - SPOC),
      b) Aktualizáciu firmwarov, operačných systémov a aplikácií pre zabezpečenie maximálnej bezpečnosti a spoľahlivosti dodaných systémov, správa licencií a certifikátov,
      c) Pravidelné pracovné stretnutia minimálne raz mesačne s účasťou projektového manažéra dodávateľa s podrobným reportingom o vykonaných zásahoch, prerokovaním problémov a plánovaním zásahov,
      d) Ad-hoc pracovné stretnutia podľa potreby na riešenie kritických incidentov,
      e) Proaktívny monitoring operačných systémov, komunikačných systémov, zálohovacích systémov a aplikácií, proaktívne riešenie bežných problémov, incidentov a vád, notifikácie kritických stavov;

   8.3. V prípade „kritickej vady“ (výpadok celého systému, výpadok dlhší ako tridsať (30) minút) sa Zhotoviteľ zaväzuje k reakčnej dobe dve (2) hod., s dobou vyriešenia bezodkladne, max. však do dvadsaťštyri (24) hod.;

   8.4. V prípade „inej ako kritickej vady“ (výpadok čiastkového komponentu, ktorý nemá vplyv na funkčnosť systému ako celku) sa Zhotoviteľ zaväzuje k reakčnej dobe max. päť (5) pracovných dní., s dobou vyriešenia najneskôr do desiatich (10) pracovných dní. Ak z objektívnych dôvodov, nezávislých od vôle Zhotoviteľa, nie je možné odstrániť vady v uvedených lehotách, vykoná sa odstránenie vady v primeranej lehote, na základe dohody medzi Objednávateľom a Zhotoviteľom. V prípade, ak nebude Zhotoviteľ schopný odstrániť vady vôbec a/alebo ich odmietne odstrániť, je Objednávateľ oprávnený zabezpečiť odstránenie vady treťou osobou na náklady Zhotoviteľa, pričom Objednávateľ je oprávnený nároky vyplývajúce zo záruky uplatniť u Zhotoviteľa;

8.5. Trvanie ZAP a SLA sa predĺži o čas potrebný na odstránenie vád; ZAP a SLA neplynie po dobu, po ktorú Objednávateľ nemôže užívať predmet plnenia pre jeho vady, za ktoré zodpovedá Zhotoviteľ. Zhotoviteľ je povinný trvale udržiavať v pohotovosti v čase vyššie definovanej dostupnosti potrebný počet pracovníkov, pre zásahy v rámci prevádzkovej a aplikačnej podpory.

Článok III.
ČAS A MIESTO PLNENIA

1. Zhotoviteľ sa zaväzuje odovzdať Objednávateľovi Diela ako celok do **desiatich (10) mesiacov od účinnosti tejto Zmluvy**.

2. Zhotoviteľ sa zaväzuje dodržať termín plnenia uvedený v bode 1. tohto článku Zmluvy tak, aby na jeho podklade mohlo byť Objednávateľovi odovzdané Dielo ako celok riadne a včas. Zhotoviteľ je oprávnený po dohode s Objednávateľom urýchliť odovzdanie Diela ako celku v prípade, ak budú dodržané všetky jeho kvalitatívne a kvantitatívne špecifiká, v súlade s touto Zmluvou.

3. Zhotoviteľ písomne alebo e-mailom informuje Objednávateľa o pripravenosti Diela alebo jeho časti na odovzdanie, a to najneskôr päť (5) pracovných dní vopred plánovaným dokončením Diela alebo jeho časti. Na základe toho Objednávateľ oznámi Zhotoviteľovi presný termín odovzdania Diela alebo jeho časti, ktorý je pre Zmluvné strany záväzný.

4. Miestom odovzdania a prevzatia Diela je sídlo Objednávateľa. O odovzdaní a prevzatí riadne dokončenej Časti diela alebo Diela ako celku bez vád a nedostatkov, a to po vykonaní všetkých skúšok nevyhnutných na preverenie funkčnosti a prevádzkyschopnosti Diela alebo jeho časti, bude spísaný Protokol o odovzdaní a prevzatí Diela alebo jeho časti (ďalej v texte len "Protokol").

5. Objednávateľ poveruje k prevzatiu Diela alebo jeho časti a k podpísaniu Protokolu Ing. Alexandra Hlavatého, vedúceho odboru informatizácie a digitalizácie a Ing. Bibiánu Paluškovú, manažérku kybernetickej a informačnej bezpečnosti. Poverené osoby sú povinné konať spoločne.

6. Protokoly podľa bodu 5. tohto článku Zmluvy budú tvoriť prílohu faktúry vystavenej Zhotoviteľom podľa článku VI. body 1. až 4. Zmluvy. Zhotoviteľ písomne alebo e-mailom informuje Objednávateľa o pripravenosti Diela alebo jeho časti na odovzdanie, na základe čoho Objednávateľ oznámi Zhotoviteľovi presný termín odovzdania Diela alebo jeho časti, ktorý je pre Zmluvné strany záväzný.

7. V prípade, že počas preberacieho konania budú zistené vady a nedostatky príslušnej časti diela a/alebo Diela ako celku, podrobný súpis zistených vád a nedostatkov bude uvedený v Protokole aj s termínom ich odstránenia. V prípade, že Objednávateľ z dôvodu zistených vád a nedostatkov príslušnej etapy Časti diela a/alebo Diela ako celku odmietne prevziať Dielo ako celok, uvedie túto skutočnosť v Protokole aj s relevantným odôvodnením a zároveň určí termín odstránenia zistených vád a nedostatkov, ktorý je Zhotoviteľ povinný akceptovať a dodržať. Po riadnom odstránení vád a nedostatkov vytknutých Objednávateľom počas preberacieho konania, z dôvodu ktorých odmietol prevziať Dielo ako celok, bude realizované opätovné preberacie konanie. Zhotoviteľ je povinný oznámiť Objednávateľovi termín opätovného preberacieho konania s tým, že ustanovenie bodu 5. tohto článku Zmluvy sa použije primerane.

8. Zhotoviteľ nie je v omeškaní s plnením predmetu tejto zmluvy po dobu, po ktorú nemohol svoje zmluvné povinnosti plniť v prípade skutočností vzniknutých z titulu vyššej moci (vis major). Zmluvné strany sa dohodli, že v prípade skutočností vis major a/alebo v prípade iných nepredvídateľných prekážok na strane Objednávateľa a/alebo na strane Zhotoviteľa, v dôsledku ktorých dôjde k prerušeniu alebo pozastaveniu prác na Diele, zmluvné strany pristúpia k uzatvoreniu dodatku k zmluve, ktorý bude obsahovať dohodu o predĺžení lehoty na dokončenie Diela s uvedením relevantných dôvodov prerušenia alebo pozastavenia prác na Diele, ako aj lehoty, v ktorej budú po odpadnutí dôvodov prerušenia alebo pozastavenia prác, práce na Diele pokračovať.

9. Nebezpečenstvo škody na Diele znáša po celú dobu realizácie Diela Zhotoviteľ. Nebezpečenstvo škody na Diele a vlastnícke právo k Dielu prechádza na Objednávateľa momentom prevzatia Diela od Zhotoviteľa v súlade s bodom 4. tohto článku Zmluvy.

Článok IV.
ĎALŠIE POVINNOSTI ZMLUVNÝCH STRÁN

1. Objednávateľ sa zaväzuje poskytovať Zhotoviteľovi všetku potrebnú súčinnosť pri zhotovovaní Diela podľa tejto zmluvy. Zhotoviteľ o poskytnutie súčinnosti požiada Objednávateľa písomne cez softwarový systém JIRA, ktorý Objednávateľ sprístupní Zhotoviteľovi v lehote najneskôr do troch (3) kalendárnych dní od nadobudnutia účinnosti tejto zmluvy a/alebo iným, zmluvnými stranami písomne dohodnutým spôsobom (ďalej v texte len „Žiadosť o poskytnutie súčinnosti"). Žiadosť o poskytnutie súčinnosti musí v každom jednotlivom prípade obsahovať údaje minimálne v rozsahu: číslo predmetnej zmluvy a podrobný popis požiadavky. Objednávateľ, podľa povahy požiadavky, zabezpečí pre Zhotoviteľa poskytnutie súčinnosti najneskôr v lehote do piatich (5) pracovných dní od doručenia žiadosti. V odôvodnených prípadoch možno lehotu podľa predchádzajúcej vety na základe vzájomnej dohody zmluvných strán primerane predĺžiť. Súčinnosť Objednávateľa so Zhotoviteľom bude dokumentovaná prostredníctvom zápisov v systéme JIRA.

2. Zhotoviteľ sa zaväzuje realizovať Dielo prostredníctvom odborných kapacít podľa jeho špecifikácie. Zoznam odborných kapacít tvorí prílohu č. 2 tejto Zmluvy.

3. Zhotoviteľ sa zaväzuje realizovať Dielo tak, aby nedošlo k narušeniu funkčnosti ostatných informačných systémov prevádzkovaných Objednávateľom. Pre realizáciu vzdialeného prístupu Zhotoviteľa k informačným systémom Objednávateľa sa Zmluvné strany dohodli, že:
   3.1. Zhotoviteľ v spolupráci s Objednávateľom zabezpečia všetky potrebné technické postupy tak, aby bolo možné bezpečne využívať službu vzdialenej správy u Objednávateľa pre potreby realizácie Predmetu plnenia;
   3.2. Zhotoviteľ zabezpečí internú evidenciu parametrov pripojenia pre vzdialenú správu v samostatnom súbore s riadeným prístupom výhradne pre ním poverené osoby, ktoré budú toto pripojenie realizovať;
   3.3. počas práce na zariadeniach Objednávateľa prostredníctvom vzdialenej správy sa Zhotoviteľ zaväzuje dodržiavať všetky zásady ochrany údajov a zariadení Objednávateľa a pre potreby spätného dohľadania a monitorovania činností, zabezpečí Zhotoviteľ vytvorenie záznamov (log súborov) o použití vzdialenej správy.

4. Zhotoviteľ je povinný strpieť výkon kontroly/auditu/overovania súvisiaceho s realizáciou Diela kedykoľvek počas platnosti a účinnosti tejto Zmluvy oprávnenými osobami a poskytnúť im všetku potrebnú súčinnosť, pričom:
   5.1. Oprávnenými osobami na výkon kontroly/auditu/overovania sú najmä:
      a) Poskytovateľ NFP a ním poverené osoby,
      b) Útvar vnútorného auditu Riadiaceho orgánu alebo Sprostredkovateľského orgánu a nimi poverené osoby,
      c) Najvyšší kontrolný úrad SR a ním poverené osoby,
      d) Orgán auditu, jeho spolupracujúce orgány (Úrad vládneho auditu) a osoby poverené na výkon kontroly/auditu,
      e) Splnomocnení zástupcovia Európskej Komisie a Európskeho dvora audítorov,
      f) Orgán zabezpečujúci ochranu finančných záujmov EÚ,
      g) Osoby prizvané orgánmi uvedenými v písmenách a) až f) v súlade s príslušnými právnymi predpismi SR a právnymi aktmi EÚ;
   5.2. Kontrolou/auditom/overovaním sa rozumie súhrn činností Poskytovateľa NFP a ním prizvaných osôb, ktorými sa overuje plnenie podmienok poskytnutia NFP v súlade so Zmluvou o poskytnutí NFP, súlad nárokovaných finančných prostriedkov/deklarovaných výdavkov a ostatných údajov predložených zo strany Objednávateľa a súvisiacej dokumentácie s právnymi predpismi SR a právnymi aktmi EÚ, dodržiavanie hospodárnosti, efektívnosti, účinnosti a účelnosti poskytnutého NFP, dôsledné a pravidelné overenie dosiahnutého pokroku Realizácie aktivít Projektu (Diela),

vrátane dosiahnutých merateľných ukazovateľov Projektu (Diela) a ďalšie povinnosti stanovené Prijímateľovi (Objednávateľovi) v Zmluve o poskytnutí NFP. Kontrola Projektu (Diela) bude vykonávaná v súlade so zákonom o finančnej kontrole a vnútornom audite a to najmä formou administratívnej kontroly kontrolovanej osoby a kontroly na mieste. V prípade, ak sú kontrolou vykonávanou formou administratívnej kontroly kontrolovanej osoby alebo kontroly na mieste identifikované nedostatky, doručí Poskytovateľ NFP Objednávateľovi návrh správy z kontroly, pričom Objednávateľ je oprávnený zaslať námietky k predmetnému návrhu v rozsahu stanovenom zákonom o finančnej kontrole a vnútornom audite. Po zohľadnení opodstatnených námietok (za predpokladu, že Objednávateľ zaslal pripomienky v stanovenej lehote) zasiela Poskytovateľ NFP Prijímateľovi (Objednávateľovi) správu z kontroly;

5.3. Zhotoviteľ sa zaväzuje, že umožní výkon kontroly/auditu zo strany oprávnených osôb na výkon kontroly/auditu v zmysle príslušných právnych predpisov SR a právnych aktov EÚ, najmä zákona o príspevku z EŠIF, zákona o finančnej kontrole a vnútornom audite a Zmluvy o poskytnutí NFP. Zhotoviteľ je počas výkonu kontroly/auditu povinný najmä preukázať oprávnenosť vynaložených výdavkov a dodržanie podmienok poskytnutia NFP v zmysle Zmluvy o poskytnutí NFP, tejto zmluvy a príslušných právnych predpisov. Zhotoviteľ je povinný zabezpečiť prítomnosť osôb zodpovedných za realizáciu predmetu zmluvy, vytvoriť primerané podmienky na riadne a včasné vykonanie kontroly/auditu, zdržať sa konania, ktoré by mohlo ohroziť začatie a riadny priebeh výkonu kontroly/auditu a plniť všetky povinnosti, ktoré mu vyplývajú najmä zo zákona o finančnej kontrole a vnútornom audite;

5.4. Zhotoviteľ je povinný uchovávať všetku dokumentáciu, a to po celú dobu povinnej archivácie týchto dokumentov, určenou v súlade s platnými právnymi predpismi SR a do tejto doby strpieť výkon kontroly/audit/overovanie zo strany oprávnených osôb. Táto doba môže byť automaticky predĺžená bez potreby vyhotovovania osobitného dodatku k tejto zmluve, a to len na základe písomného oznámenia Objednávateľa Zhotoviteľovi o tom, že nastali skutočnosti uvedené v článku 140 všeobecného nariadenia Európskeho parlamentu a Rady EÚ č. 1303/2013 zo 17. decembra 2013, a to o čas trvania týchto skutočností. Poskytovateľ NFP je oprávnený prerušiť plynutie lehôt vo vzťahu k výkonu kontroly žiadosti o platbu formou administratívnej kontroly pred jej uhradením/zúčtovaním v prípadoch stanovených článkom 132 ods. 2 všeobecného nariadenia. Zhotoviteľ je povinný prijať opatrenia na nápravu nedostatkov zistených kontrolou/auditom v zmysle správy z kontroly/auditu v lehote stanovenej oprávnenými osobami na výkon kontroly/auditu.

6. Zhotoviteľ sa zaväzuje rešpektovať a dodržiavať pokyny Objednávateľa pri plnení Predmetu zmluvy. Súčasne sa zaväzuje dodržiavať pokyny Poskytovateľa NFP v zmysle Zmluvy o poskytnutí NFP uzatvorenej medzi Objednávateľom ako prijímateľom NFP a Poskytovateľom NFP a na tento účel poskytnúť všetku dokumentáciu, prípadne vysvetlenia a vyžiadané podklady Objednávateľom pre Poskytovateľa NFP.

7. Vzhľadom na skutočnosť, že Zmluva o poskytnutí NFP uzatvorená medzi Objednávateľom a Poskytovateľom NFP na predmet plnenia podľa tejto zmluvy, jej prílohy a Všeobecné zmluvné podmienky prislúchajúce k tejto zmluve o NFP (ďalej len „VZP") sú povinne zverejňované v zmysle § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov (ďalej ako „zákon o slobodnom prístupe k informáciám"), Zmluvné strany sa dohodli, že v prípade zmeny Zmluvy o poskytnutí NFP a jej príloh z dôvodu ich aktualizácie a zosúladenia, je Objednávateľ povinný písomne oznámiť túto zmenu Zhotoviteľovi, spolu s odkazom na číslo, pod ktorým bude aktualizovaná Zmluva o poskytnutí NFP a jej prílohy zverejnené v Centrálnom registri zmlúv alebo na webovej stránke Poskytovateľa NFP.

8. Objednávateľ je povinný bez zbytočného odkladu písomne upovedomiť Zhotoviteľa o všetkých zmenách podľa bodu 6. tohto článku Zmluvy a Zhotoviteľ je povinný sa s aktuálne platným znením všetkých dokumentov oboznámiť a postupovať podľa nich pri plnení predmetu tejto Zmluvy. Zmluvné strany sa dohodli, že v prípade zmien, ktoré budú mať zásadný vplyv na plnenie predmetu tejto Zmluvy, alebo to bude vyplývať zo Zmluvy o poskytnutí NFP, zmeny budú upravené formou písomných dodatkov k tejto

Zmluve. Za zásadné zmeny sa považujú zmena spôsobu financovania Poskytovateľom NFP, zníženie alokovaných prostriedkov na Výzvu, odstúpenie Poskytovateľa NFP od Zmluvy.

9. Zhotoviteľ sa zaväzuje vykonať Predmet plnenia v rozsahu špecifikovanom v článku II. tejto Zmluvy vo vlastnom mene, na vlastné náklady, na vlastné nebezpečenstvo a na vlastnú zodpovednosť. Ak bude časť Predmetu zmluvy vykonávaná iným subjektom v mene Zhotoviteľa (subdodávateľom), Zhotoviteľ sa zaväzuje predložiť Objednávateľovi zoznam subdodávateľov, v ktorom v zmysle zákona o verejnom obstarávaní uvedie údaje o všetkých známych subdodávateľoch, údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia. Zoznam subdodávateľov zadefinovaných pri podpise Zmluvy, spolu s uvedením predmetu a rozsahu subdodávky, tvorí prílohu č. 3 tejto Zmluvy.

10. Zhotoviteľ v prípade, ak bude mať záujem zadať určitú časť Predmetu plnenia ďalšiemu subdodávateľovi, ktorý nebol definovaný v zozname subdodávateľov pri podpise tejto Zmluvy, resp. ak bude mať záujem zmeniť subdodávateľa uvedeného v Zozname subdodávateľov pri podpise tejto Zmluvy, počas plnenia Predmetu zmluvy, je oprávnený zmeniť subdodávateľa len s predchádzajúcim písomným súhlasom Objednávateľa. Žiadosť o zmenu subdodávateľa písomne predkladá Zhotoviteľ Objednávateľovi najneskôr päť (5) pracovných dní pred plánovaným dátumom zmeny subdodávateľa. V prípade súhlasu Objednávateľa so zmenou subdodávateľa, Zmluvné strany upravia túto skutočnosť v rozsahu údajov uvedených v bode 8. tohto článku Zmluvy, a to formou dodatku k tejto Zmluve.

11. Objednávateľ si vyhradzuje právo kedykoľvek počas realizácie Diela odmietnuť subdodávateľa Zhotoviteľa. Zhotoviteľ je v danom prípade povinný bezodkladne vykonať všetky potrebné úkony na to, aby s odmietnutým subdodávateľom ukončil spoluprácu na realizácii Diela.

12. Zhotoviteľ je povinný plniť všetky povinnosti, ktoré mu vyplývajú zo zákona o verejnom obstarávaní a zákona č. 343/2015 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, a to najmä:
    a) prostredníctvom oprávnenej osoby viesť a udržiavať svoj aktuálny záznam v registri partnerov verejného sektora,
    b) zabezpečiť splnenie povinnosti podľa písm. a) u každého svojho subdodávateľa a navrhovaného subdodávateľa.

13. Zhotoviteľ je povinný uzatvoriť zmluvu o poistení proti rizikám obvyklým pre dohodnutý predmet Zmluvy na ochranu Objednávateľa, svoju finančnú ochranu, alebo ochranu svojich subdodávateľov, proti akejkoľvek strate, škode alebo zodpovednosti spojenej s realizáciou Diela a/alebo súvisiacej s ňou, s výškou poistného plnenia minimálne do výšky ceny za Dielo (ďalej len „**Zmluva o poistení**").

14. Zmluvu o poistení a doklad o úhrade poistnej sumy predloží Zhotoviteľ Objednávateľovi najneskôr v deň podpisu tejto Zmluvy. Zhotoviteľ je povinný zabezpečiť platnosť a účinnosť Zmluvy o poistení po celú dobu realizácie Diela. V prípade, ak Objednávateľ poskytne Zhotoviteľovi pri podpise tejto zmluvy dodatočnú lehotu na predloženie zmluvy o poistení a dokladu o úhrade poistnej sumy, pričom ani v tejto dodatočne poskytnutej lehote nie dlhšej ako päť (5) pracovných dní odo dňa nadobudnutia účinnosti Zmluvy Zhotoviteľ požadované doklady nepredloží, uvedená skutočnosť zakladá oprávnenie Objednávateľa na odstúpenie od tejto Zmluvy.

15. Zhotoviteľ je povinný bezodkladne (najneskôr do dvadsaťštyri (24) hodín) informovať Objednávateľa o vzniku poistných udalostí súvisiacich s realizáciou Diela. Objednávateľ je kedykoľvek počas realizácie Diela oprávnený požadovať od Zhotoviteľa potvrdenie poisťovne o trvaní a rozsahu poistenia.

16. Zmluvné strany sú povinné dodržiavať zásady informačnej bezpečnosti, pričom:
    16.1. Zhotoviteľ je povinný dodržiavať všetky povinnosti a obmedzenia vyplývajúce zo zákona č. 18/2018 Z.z. o ochrane osobných údajov v znení neskorších predpisov.

16.2. Zmluvné strany sa zaväzujú dodržiavať zásady informačnej bezpečnosti podľa medzinárodných štandardov. Zhotoviteľ prehlasuje, že prijal technické a organizačné opatrenia na zabezpečenie:

a) kontroly prístupu k zariadeniam, aby sa zabránilo neoprávnenému prístupu k zariadeniu na prístup k osobným údajom z informačného systému Objednávateľa,
b) kontroly postupov a technických zariadení, aby sa zabránilo neoprávnenému vkladaniu osobných údajov do informačného systému a neoprávnenému prehliadaniu osobných údajov, pozmeňovaniu osobných údajov alebo vymazaniu osobných údajov v systémoch Objednávateľa zo strany Zhotoviteľa,
c) kontroly postupov a technických zariadení, aby sa zabránilo použitiu systémov automatizovaného spracúvania osobných údajov neoprávnenými osobami pomocou zariadenia na prenos osobných údajov,
d) kontroly prenosu údajov, aby sa zabezpečila možnosť overiť a zistiť subjekty, ktorým sa preniesli osobné údaje nachádzajúce sa v informačných systémoch Objednávateľa,
e) kontroly vkladania údajov do informačných systémov Objednávateľa, aby sa zabezpečilo, že bude možné overiť a zistiť, aké osobné údaje sa vložili do informačného systému Objednávateľa a kedy a kto ich tam vložil,
f) obnovy osobných údajov, aby sa zabezpečilo, že sa inštalované informačné systémy Objednávateľa obnovia, ak dôjde k ich prerušeniu.

16.3. Zhotoviteľ prehlasuje, že všetky jemu poskytnuté osobné údaje z informačných systémov Objednávateľa vráti Objednávateľovi bezodkladne po dodaní Diela a všetky ich kópie zlikviduje, pokiaľ nie je medzi Zmluvnými stranami dohodnuté inak.

16.4. Poverená osoba Zhotoviteľa realizujúca činnosti spojené s Predmetom plnenia (akoukoľvek formou) u Objednávateľa je povinná najmä zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku pri prácach s informačnými systémami Objednávateľa.

Článok V.
CENA ZA DIELO

1. Dohodnutá cena (odplata) v prospech Zhotoviteľa za riadne dodanie Predmetu plnenia je stanovená v súlade so zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov a v súlade s výsledkom verejného obstarávania, na základe predloženej cenovej ponuky Zhotoviteľa. Súťažná cenová ponuka Zhotoviteľa tvorí prílohu č. 4, ktorá je neoddeliteľnou súčasťou tejto Zmluvy.

2. Dohodnutá cena (odplata) v prospech Zhotoviteľa za riadne dodanie Predmetu plnenia predstavuje sumu v celkovej výške 297 120,00 eur bez DPH (slovom: dvestodeväťdesiatsedemtisícstodvadsať eur), DPH 23 % 68 337,60 eur, spolu s DPH 365 457,60 eur (slovom: tristošesťdesiatpäťtisícštyristopäťdesiatsedem eur a šesťdesiat centov) v nasledovnej štruktúre:

P.č.	Názov položky	Cena bez DPH (EUR)	DPH (EUR)	Cena spolu s DPH (EUR)
1	Vypracovanie relevantnej bezpečnostnej dokumentácie; (pre všetky Časti diela podľa článku I. bod 1. písm. a) tejto Zmluvy)	45 250,00	10 407,50	55 657,50
2	Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica; (pre všetky Časti diela podľa článku I. bod 1. písm. b) tejto Zmluvy)	48 430,00	11 138,90	59 568,90
3	Vykonanie segmentácie siete Mesta Banská Bystrica s ohľadom na			

	súčasné prevádzkové požiadavky; (pre všetky Časti diela podľa článku I. bod 1. písm. c) tejto Zmluvy)	25 900,00	5 957,00	31 857,00
4	Zrealizovanie výmeny aktívnych prvkov core časti siete; (pre všetky Časti diela podľa článku I. bod 1. písm. d) tejto Zmluvy)	110 760,00	25 474,80	136 234,80
5	Implementovanie systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete; (pre všetky Časti diela podľa článku I. bod 1. písm. e) tejto Zmluvy)	35 340,00	8 128,20	43 468,20
6	Implementovanie riešenia centrálneho bezpečnostného manažmentu pre koncové stanice; (pre všetky Časti diela podľa článku I. bod 1.1 písm. f) tejto Zmluvy)	31 440,00	7 231,20	38 671,20
	SPOLU	**297 120,00**	**68 337,60**	**365 457,60**

(ďalej v texte len „**Cena za Dielo**").

3. Zhotoviteľ upozorní na skutočnosť, že je, alebo nie je platcom DPH. Ak sa zhotoviteľ stane platcom DPH počas trvania Zmluvy, Cena za Dielo dohodnutá v Zmluve nebude zvýšená, bude upravená na základ dane a sadzbu DPH podľa príslušného právneho predpisu upravujúceho výšku DPH.

4. V prípade, že počas platnosti a účinnosti tejto Zmluvy dôjde k legislatívnym zmenám, vzťahujúcim sa k zmene príslušnej sadzby DPH podľa zákona č.222/2004 Z.z. o dani z pridanej hodnoty v znení neskorších predpisov, Zmluvné strany sa dohodli, že takáto zmena nie je zmenou Zmluvy a podkladom pre fakturáciu je Cena za Dielo bez DPH a príslušná sadzba DPH v zmysle platnej legislatívy.

5. Cena za Dielo je konečná a zahŕňa akékoľvek a všetky účelne vynaložené náklady a výdavky Zhotoviteľa súvisiace s plnením podľa tejto Zmluvy.

6. Zmluvné strany sa dohodli, že Objednávateľ neposkytne Zhotoviteľovi akýkoľvek preddavok resp. akúkoľvek zálohovú platbu vopred požadovanú zhotoviteľom.

7. Zhotoviteľ nie je oprávnený požadovať zvýšenie ceny za Dielo, ak k zvýšeniu nákladov na zhotovenie Diela došlo z dôvodov na strane Zhotoviteľa, v dôsledku porušenia a/alebo nedodržania podmienok realizácie Diela vyplývajúcich Zhotoviteľovi z Podkladovej dokumentácie a/alebo z tejto Zmluvy. V prípade vzniku potreby zníženia rozsahu realizácie Diela, Objednávateľ je oprávnený cenu za Dielo znížiť o hodnotu nerealizovanej časti Diela.

8. Zhotoviteľ deklaruje, že sa včas a riadne oboznámil s rozsahom a charakterom predmetu plnenia podľa tejto Zmluvy, a zároveň, že pred vypracovaním súťažnej cenovej ponuky Zhotoviteľa:
   a) sa podrobne oboznámil s Podkladovou dokumentáciou a návrhom tejto Zmluvy,
   b) v kalkulácii Ceny za Dielo zohľadnil najmä, nie však výlučne, všetky ekonomické a technické podmienky zhotovenia Diela, ako aj termíny jednotlivých plnení, v kontexte Podkladovej dokumentácie a tejto Zmluvy.

Článok VI.
PLATOBNÉ PODMIENKY

1. Na základe dohody Zmluvných strán, Cena za Dielo bude uhradená na základe faktúry vystavenej Zhotoviteľom. Cena za Dielo bude uhradená po dodaní Diela alebo Časti diela a jeho prevzatí Objednávateľom spôsobom podľa článku III. bod 4. Zmluvy.

2. Zmluvné strany sa dohodli, že v prípade, ak budú jednotlivé Časti diela Zhotoviteľom dodané a Objednávateľom prevzaté samostatne podľa článku III. bod 4. Zmluvy, je Zhotoviteľ oprávnený vystaviť faktúru za čiastkové plnenie Predmetu plnenia nasledovne:
   a) na prvú časť Ceny za Dielo, pričom hodnota ukončenej a prevzatej Časti diela dosiahne minimálne 40% z celkovej Ceny za Dielo,
   b) na druhú časť Ceny za Dielo až po ukončení a prevzatí Diela ako celku Objednávateľom.

3. Zhotoviteľ je oprávnený fakturovať cenu za Dielo alebo jej časť v lehote do siedmich (7) pracovných dní odo dňa podpísania Protokolu o odovzdaní a prevzatí Diela alebo jeho časti.

4. Zhotoviteľom vystavené faktúry podľa bodu 2. a 3. tohto článku Zmluvy musia byť vystavené v štyroch (4) originálnych vyhotoveniach a musia obsahovať všetky údaje podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov, zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov. Prílohu každej faktúry bude tvoriť ocenený súpis a príslušný Protokol o odovzdaní a prevzatí Diela alebo Časti diela.

5. Objednávateľ výslovne súhlasí so zaslaním faktúry v elektronickej forme, a to na e-mailovú adresu Objednávateľa podatelna@banskabystrica.sk. Faktúra sa považuje za doručenú, dňom jej riadneho doručenia na e-mailovú adresu Objednávateľa.

6. V prípade, že Zhotoviteľom vystavené faktúry na zaplatenie Ceny za Dielo alebo jej časti budú obsahovať nesprávne a/alebo neúplné údaje, Objednávateľ je oprávnený vrátiť ich v lehote splatnosti Zhotoviteľovi na prepracovanie, s uvedením vytýkaných nedostatkov. Zhotoviteľ je povinný Objednávateľom vrátené faktúry podľa charakteru ich nedostatku opraviť alebo vystaviť nové. Vrátením faktúr Zhotoviteľovi neplynie lehota ich splatnosti. Nová lehota splatnosti začína plynúť dňom doručenia nových alebo opravených faktúr. V pochybnostiach sa má za to, že Zhotoviteľom vystavené faktúry boli doručené Objednávateľovi na tretí deň po ich odoslaní Zhotoviteľom.

7. Cena za Dielo bude financovaná z prostriedkov Európskych štrukturálnych a investičných fondov v rámci Operačného programu Program Slovensko (PSK). Zhotoviteľom vystavené faktúry na zaplatenie ceny za Dielo podliehajú režimu schvaľovania Riadiacim orgánom (RO)/Sprostredkovateľským orgánom (SO) podľa Zmluvy o poskytnutí nenávratného finančného príspevku uzatvorenej medzi Objednávateľom a Poskytovateľom NFP (ďalej v texte len "**Zmluva o poskytnutí NFP**"). Zhotoviteľom vystavené faktúry na zaplatenie ceny za Dielo budú splatné do šesťdesiat (60) kalendárnych dní od ich riadneho doručenia Objednávateľovi. V prípade, že v lehote splatnosti faktúr na zaplatenie ceny za Dielo nebudú finančné prostriedky poskytované príslušným RO/SO pre PSK pripísané na účet Objednávateľa uvedený v záhlaví tejto zmluvy, Zhotoviteľ bez akýchkoľvek výhrad akceptuje a súhlasí s tým, že Objednávateľ nebude v omeškaní s úhradou ceny za Dielo, ak fakturované sumy uhradí v lehote do piatich (5) pracovných dní odo dňa pripísania finančných prostriedkov poskytnutých príslušným RO/SO PSK na účet Objednávateľa.

8. V prípade, že Zhotoviteľ má účet vedený v banke mimo územia SR, bude znášať všetky poplatky za bezhotovostný styk spojený s úhradou záväzkov, vyplývajúcich z plnenia tejto Zmluvy v plnej výške. V takom prípade bude Objednávateľ postupovať v súlade s § 24 zákona o účtovníctve a pri prevode peňažných prostriedkov v cudzej mene z účtu Objednávateľa zriadeného v eurách na účet Zhotoviteľa zriadeného v cudzej mene. Objednávateľ použije kurz banky platný v deň odpísania prostriedkov z účtu Objednávateľa, tzn. v deň uskutočnenia účtovného prípadu. Týmto kurzom prepočítaný výdavok na eurá bude uhradený Zhotoviteľovi. V prípade prevodu peňažných prostriedkov v cudzej mene z účtu Objednávateľa zriadeného v cudzej mene na účet Zhotoviteľa v rovnakej cudzej mene použije Objednávateľ referenčný výmenný kurz určený a vyhlásený Európskou centrálnou bankou v deň predchádzajúci dňu uskutočnenia účtovného prípadu (odpísania prostriedkov). Týmto kurzom prepočítaný výdavok na eurá bude uhradený Objednávateľovi.

Článok VII.
ZODPOVEDNOSŤ ZA VADY A ZÁRUČNÁ DOBA

1. Zhotoviteľ zodpovedá za to, že Dielo bude vykonané v rozsahu, za podmienok a v kvalite vyplývajúcej z Podkladovej dokumentácie a z ustanovení tejto Zmluvy a bude vyhovovať požiadavkám stanoveným Objednávateľom a platnými všeobecne záväznými právnymi predpismi.

2. Zhotoviteľ zodpovedá za vady Diela, ktoré má Dielo v čase jeho odovzdania Objednávateľovi, ak boli preukázateľne spôsobené s porušením povinnosti Zhotoviteľa a v rozsahu záruky Diela poskytnutej v zmysle tejto Zmluvy. Zhotoviteľ nezodpovedá za vady spôsobené nevhodnými pokynmi Objednávateľa a/alebo inej Objednávateľom poverenej osoby, ak Zhotoviteľ písomne upozornil Objednávateľa na nevhodnú povahu jeho pokynov a Objednávateľ na použití pokynov pri vykonávaní Diela písomne trval, alebo ak Zhotoviteľ túto nevhodnosť nemohol ani pri náležitej odbornej starostlivosti zistiť.

3. Zhotoviteľ poskytne záručnú dobu na Dielo v rozsahu šesťdesiat (60) mesiacov odo dňa prevzatia riadne dokončeného Diela ako celku bez vád a nedostatkov Objednávateľom na základe Protokolu podľa článku III. bod 4., 6. a 7. Zmluvy tejto Zmluvy. Ustanovenie predchádzajúcej vety sa nepoužije v prípade zabudovaných komponentov, pri ktorých výrobcovia poskytujú v záručných listoch kratšie záručné doby, a ktoré je Zhotoviteľ povinný akceptovať, v takomto prípade je záručná doba minimálne dvadsaťštyri (24) mesiacov.

4. Objednávateľ sa zaväzuje, že vady Diela uplatní u Zhotoviteľa bezodkladne po ich zistení, a to cez softwarový systém JIRA a/alebo iným, Zmluvnými stranami písomne dohodnutým spôsobom. Oznámenie Objednávateľa o vade Diela musí obsahovať: a) číslo zmluvy a b) označenie a popis vady (ďalej v texte len „**Oznámenie o vade**“).

5. Zhotoviteľ je povinný preveriť reklamovanú vadu Diela bezodkladne najneskôr do dvadsaťštyri (24) hodín po doručení Oznámenia o vade a vyhotoviť záznam reklamovanej vady.

6. V prípade
   a) vzniku vád Diela, ktoré nebránia riadnemu užívaniu a prevádzkyschopnosti Diela, je Zhotoviteľ povinný začať s odstraňovaním reklamovaných vád Diela najneskôr do piatich (5) pracovných dní od doručenia Oznámenia o vade; Zhotoviteľ je povinný zabezpečiť odstránenie takýchto vád Diela v čo najkratšom možnom termíne, najneskôr do desiatich (10) pracovných dní od doručenia Oznámenia o vade;
   b) vzniku kritických systémových porúch, t.j. vád, ktoré majú podstatný vplyv na funkčnosť a prevádzkyschopnosť Diela, je Zhotoviteľ povinný začať s odstraňovaním reklamovaných vád Diela bezodkladne, najneskôr však do dvoch (2) hodín od doručenia Oznámenia o vade Zhotoviteľovi; Zhotoviteľ je povinný zabezpečiť odstránenie takýchto vád Diela v čo najkratšom možnom termíne, najneskôr však do dvadsaťštyri (24) hodín od doručenia Oznámenia o vade; Zhotoviteľ je zároveň povinný urobiť všetky opatrenia, aby bola bezodkladne zabezpečená prevádzkyschopnosť Diela.

7. V prípade omeškania sa Zhotoviteľa so začatím odstraňovania reklamovaných vád Diela alebo s ich odstránením, alebo ak Zhotoviteľ odmietne reklamované vady odstrániť, Objednávateľ je oprávnený zabezpečiť odstránenie reklamovaných vád na náklady Zhotoviteľa.

8. O termíne a spôsobe odstránenia vady Diela je Zhotoviteľ povinný Objednávateľa bezodkladne informovať a to cez softwarový systém JIRA a/alebo iným, Zmluvnými stranami písomne dohodnutým spôsobom.

9. V prípade objektívnej nemožnosti dodržania termínov stanovených v bode 6. a 7. tohto článku Zmluvy (napr.: v dôsledku živelnej pohromy, zložitého a/alebo náročného procesu odstránenia vady Diela a pod.), Zhotoviteľ je povinný Objednávateľa o tejto skutočnosti bezodkladne informovať, a to cez softwarový systém JIRA a/alebo iným, zmluvnými stranami písomne dohodnutým spôsobom. Zhotoviteľ je v takom

prípade zároveň povinný oznámiť Objednávateľovi predpokladaný časový rámec odstránenia vady Diela. O odstránení vady je zhotoviteľ povinný Objednávateľa bezodkladne informovať.

10. Zmluvná strana, ktorá svojim konaním alebo nekonaním a/alebo porušením, prípadne zanedbaním niektorej z povinností vyplývajúcich z tejto Zmluvy zavinila vznik škody, je povinná nahradiť škodu, ktorá v dôsledku toho vznikla druhej Zmluvnej strane. Práva Zmluvných strán na náhradu škody sa v častiach neupravených touto Zmluvou riadia príslušnými všeobecne záväznými právnymi predpismi, pričom sa uhrádza len skutočná škoda.

Článok VIII.
PORUŠENIE POVINNOSTÍ

1. V prípade, že Zhotoviteľ poruší svoju zmluvnú povinnosť, na plnenie ktorej sa zaviazal v článku III. bod 1. tejto Zmluvy, Objednávateľ je oprávnený uplatniť si voči Zhotoviteľovi nárok na zaplatenie zmluvnej pokuty vo výške 300,00 eur (slovom: tristo eur) za každý aj začatý deň omeškania s plnením.

2. V prípade, že Zhotoviteľ poruší svoju zmluvnú povinnosť, na plnenie ktorej sa zaviazal v článku VII. bod 6 písm. a) tejto Zmluvy, Objednávateľ je oprávnený uplatniť si voči Zhotoviteľovi nárok na zaplatenie zmluvnej pokuty vo výške 100,00 eur (slovom: jednosto eur) za každý aj začatý deň omeškania s odstránením vady a za každú vadu samostatne.

3. V prípade, že Zhotoviteľ poruší svoju zmluvnú povinnosť, na plnenie ktorej sa za viazal v článku VII. bod 6. písm. b) tejto Zmluvy, Objednávateľ je oprávnený uplatniť si voči Zhotoviteľovi nárok na zaplatenie zmluvnej pokuty vo výške 300,00 eur (slovom: tristo eur) za každý aj začatý deň omeškania s odstránením vady a za každú vadu samostatne.

4. V prípade, že Zhotoviteľ poruší svoju zmluvnú povinnosť, na plnenie ktorej sa zaviazal v článku IX. bod 4. tejto Zmluvy, Objednávateľ je oprávnený uplatniť si voči Zhotoviteľovi nárok na zaplatenie zmluvnej pokuty vo výške 1 000,00 eur (slovom: jedentisíc eur) za každý aj začatý deň omeškania so splnením jeho zmluvnej povinnosti.

5. Zmluvné strany považujú dohodnutú výšku zmluvnej pokuty za primeranú, zodpovedajúcu povahe a rozsahu zabezpečovaných zmluvných povinností. Splnením záväzku zaplatiť zmluvnú pokutu nezanikajú povinnosti zmluvnej strany, plnenie ktorých je zabezpečené dohodou o zmluvnej pokute.

6. Dohodou o zmluvnej pokute nie je dotknuté právo Zmluvných strán na náhradu škody. V prípade vzniku škody je ktorákoľvek zo Zmluvných strán oprávnená nárokovať si jej náhradu vo výške presahujúcej výšku zmluvnej pokuty.

7. Objednávateľ má právo, pri uplatňovaní zmluvných pokút a/alebo iných peňažných nárokov voči Zhotoviteľovi, započítať takéto pohľadávky jednostranným právnym úkonom s akoukoľvek (aj nesplatnou) pohľadávkou Zhotoviteľa voči Objednávateľovi.

8. Zhotoviteľ nie je oprávnený započítať svoje pohľadávky alebo nároky voči Objednávateľovi oproti pohľadávkam alebo nárokom Objednávateľa voči Zhotoviteľovi.

9. Zhotoviteľ nie je oprávnený previesť svoje práva a povinnosti vyplývajúce z tejto Zmluvy alebo ich časť na tretiu osobu. Zhotoviteľ tiež nie je oprávnený postúpiť a ani založiť akékoľvek svoje pohľadávky vzniknuté voči Objednávateľovi na základe a/alebo v súvislosti s touto Zmluvou a/alebo v súvislosti s plnením záväzkov podľa tejto Zmluvy.

10. V prípade, ak riadiaci orgán/sprostredkovateľský orgán alebo iný oprávnený orgán udelí Objednávateľovi v súvislosti s omeškaním, neplnením projektu a termínov, ktoré spôsobil priamo alebo nepriamo Zhotoviteľ finančnú opravu, Objednávateľ je oprávnený uplatniť si tento nárok u Zhotoviteľa, pričom tento je povinný ho na základe výzvy Objednávateľa uhradiť v lehote stanovenej Objednávateľom.

Článok IX.
DOBA TRVANIA A ZÁNIK ZMLUVY

1. Táto Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch Zmluvných strán a účinnosť dňom nasledujúcim po jej zverejnení v Centrálnom registri zmlúv v súlade s ust. § 5a ods.1 zákona č. 211/2000 Z.z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov v spojení s ust. § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a súčasne splnením odkladacej podmienky, ktorou je schválenie zákazky, ktorá je predmetom tejto Zmluvy v rámci kontroly verejného obstarávania, t. j. dňom doručenia správy z kontroly verejného obstarávania Objednávateľovi ako prijímateľovi nenávratného finančného príspevku. O splnení odkladacej podmienky je Objednávateľ povinný bezodkladne informovať Zhotoviteľa.

2. Táto Zmluva zanikne:
   2.1. splnením predmetu zmluvy;

   2.2. dohodou Zmluvných strán ku dňu uvedenému v dohode; Zmluvné strany v uzatvorenej dohode zároveň upravia usporiadanie všetkých vzájomných nárokov vzniknutých a/alebo vyplývajúcich z tejto Zmluvy;

   2.3. odstúpením od Zmluvy z dôvodu podstatného porušenia tejto Zmluvy, pričom o podstatné porušenie Zmluvy pôjde v prípade, ak Zhotoviteľ, aj napriek písomnému upozorneniu Objednávateľa s upozornením na možnosť odstúpenia od Zmluvy, opakovane poruší svoje zmluvné povinnosti na splnenie ktorých sa zaviazal v zmysle článku III. bod 1., článku IV bod 2., bod 3., bod 4., bod. 12. a bod 16.4. tejto Zmluvy;

   2.4. odstúpením Objednávateľa od Zmluvy v prípade, ak v priebehu platnosti a účinnosti tejto Zmluvy vstúpi Zhotoviteľ do likvidácie, alebo bude na majetok Zhotoviteľa vyhlásený konkurz alebo povolená reštrukturalizácia, alebo ak bude Zhotoviteľ preukázateľne spĺňať zákonné podmienky na začatie konkurzného alebo reštrukturalizačného konania, v zmysle zákona č. 7/2005 Z.z. o konkurze a reštrukturalizácii v znení neskorších predpisov;

   2.5. odstúpením Objednávateľa od Zmluvy v prípade, ak výsledky kontroly dokumentácie verejného obstarávania Riadiacim orgánom pre OPII resp. Úradom pre verejné obstarávanie neumožňujú financovanie výdavkov vzniknutých z tohto obstarávania;

   2.6. odstúpením Objednávateľa od Zmluvy v prípade neschválenia ŽoNFP projektu.

3. Odstúpením od Zmluvy zanikajú všetky práva a povinnosti Zmluvných strán vyplývajúce z tejto zmluvy, s výnimkou práv na zmluvné a zákonné sankcie (napr. právo na náhradu škody, právo na zmluvnú pokutu, atď.) a s výnimkou zmluvných ustanovení, ktoré na základe prejavu vôle zmluvných strán alebo z dôvodu ich právnej povahy zostávajú v platnosti aj po skončení platnosti a účinnosti tejto zmluvy.

4. V prípade zániku zmluvy z dôvodov podľa bodu 2.3. alebo 2.4. tohto článku Zmluvy, Zhotoviteľ je povinný najneskôr do troch (3) pracovných dní od skončenia platnosti a účinnosti tejto Zmluvy protokolárne odovzdať Objednávateľovi zhotovenú Časť diela, všetky veci a doklady prevzaté od Objednávateľa za účelom zhotovenia Diela, ako aj potvrdenia a doklady týkajúce sa časti Diela zhotoveného a odovzdaného ku dňu skončenia platnosti a účinnosti Zmluvy.

5. V prípade zániku zmluvy z dôvodov podľa bodu 2.3. alebo 2.4. tohto článku Zmluvy, Zhotoviteľ je povinný v lehote do desiatich (10) dní od zániku Zmluvy, predložiť Objednávateľovi vyúčtovanie Ceny za Dielo v rozsahu nákladov skutočne vynaložených na zhotovenie Diela ku zániku. V prípade, že Objednávateľ neodsúhlasí vyúčtovanie ceny za Dielo predložené Zhotoviteľom podľa predchádzajúcej vety, za účelom stanovenia ceny za Dielo zhotovené ku dňu zániku zmluvy, si Objednávateľ vyhradzuje právo zadať vypracovanie znaleckého posudku, a to na náklady Zhotoviteľa.

Článok X.
DORUČOVANIE

1. Pokiaľ v zmluve nie je výslovne uvedené inak, všetky písomnosti v zmysle tejto zmluvy budú doručované prostredníctvom: a) poštovej prepravy doporučenou zásielkou, b) kuriérskej služby alebo c) e-mailom. Písomnosti, z povahy ktorých vyplýva potreba ich písomného doručenia, budú doručované prostredníctvom poštovej prepravy doporučenou zásielkou alebo kuriérskou službou.

2. Písomnosti sa považujú za riadne doručené ich preukázaným doručením na adresy Zmluvných strán uvedené v záhlaví Zmluvy, alebo odmietnutím ich prevzatia, v prípade odosielania e-mailom, tieto sa považujú za riadne doručené po ich preukázanom odoslaní.

3. Písomnosti sa doručujú doporučene na adresu sídla Zmluvnej strany uvedenú v záhlaví tejto Zmluvy. Každá zo Zmluvných strán je povinná oznámiť druhej Zmluvnej strane každú zmenu svojich identifikačných a kontaktných údajov a to najneskôr do troch (3) pracovných dní odo dňa vzniku zmeny.

4. Zásielka obsahujúca písomnosť sa považuje za doručenú dňom, keď sa dostane do sféry dispozície Zmluvnej strany, ktorej je adresovaná, hoci táto si ju fyzicky neprevezme alebo aj v prípade, ak ju Zmluvná strana, ktorej je zásielka adresovaná, odmietne bezdôvodne prevziať. Zásielka sa považuje za doručenú aj v prípade, ak ju pošta, resp. iný doručovateľ vráti z akýchkoľvek dôvodov nemožnosti doručenia odosielajúcej zmluvnej strane, hoci táto ju doručovala na poslednú známu adresu druhej Zmluvnej strany, určenú v súlade s ustanoveniami tejto Zmluvy. Zásielka sa v tomto prípade považuje za doručenú nasledujúcim dňom po dni jej vrátenia odosielajúcemu.

5. V prípade elektronického doručovania medzi právnickými osobami na aktivované elektronické schránky pre doručovanie, riadia sa pravidlá doručovania vždy aktuálne platnou legislatívou upravujúcou podmienky a pravidlá doručovania medzi právnickými osobami na ich aktivované elektronické schránky pre doručovanie.

Článok XI.
DÔVERNOSŤ INFORMÁCIÍ A ZÁVÄZOK MLČANLIVOSTI

1. Zmluvné strany sa zaväzujú, že všetky písomné a/alebo elektronické výstupy súvisiace s plnením predmetu tejto Zmluvy budú použité výlučne v záujme splnenia účelu tejto Zmluvy a v súlade s platnými právnymi predpismi Slovenskej republiky. Akékoľvek technické, personálne alebo obchodné informácie, informácie o metódach poskytovania služieb a/alebo znalostné informácie, s ktorými sa Zmluvné strany oboznámia v súvislosti s plnením predmetu tejto zmluvy, majú dôverný charakter (ďalej v texte len „**dôverné informácie**“) a ich oznámenie tretím osobám, ako aj ich zverejnenie, podlieha predchádzajúcemu písomnému súhlasu dotknutej zmluvnej strany. Tým nie sú dotknuté ustanovenia príslušných platných právnych predpisov Slovenskej republiky, ktoré umožňujú v osobitných prípadoch poskytnutie informácií aj bez súhlasu dotknutej Zmluvnej strany.

2. Zmluvné strany sa zaväzujú, že bez predchádzajúceho písomného súhlasu druhej Zmluvnej strany, nepoužijú dôverné informácie pre seba alebo pre tretie osoby, neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k dôverným informáciám. Za tretie osoby sa nepokladajú členovia orgánov zmluvných strán, audítori alebo právni poradcovia zmluvných strán, ktorí sú v rozsahu sprístupnených informácií viazaní povinnosťou mlčanlivosti na základe všeobecne záväzných právnych predpisov.

3. Záväzok zmluvných strán podľa bodu 1. a 2. tohto článku Zmluvy trvá aj po ukončení platnosti a účinnosti tejto Zmluvy.

4. Záväzok zmluvných strán podľa bodu 1. a 2. tohto článku Zmluvy sa nevzťahuje na prípady, ak:
   a) je informácia verejne dostupná z iného dôvodu, ako je porušenie povinnosti mlčanlivosti dotknutou Zmluvnou stranou,

b) je informácia poskytnutá so súhlasom druhej Zmluvnej strany,
c) ide o povinnosť poskytnúť informácie, stanovenú na základe všeobecne záväzných právnych predpisov.

5. Zmluvné strany sa zaväzujú navzájom si oznámiť každú neoprávnenú manipuláciu s dôvernými informáciami (ďalej v texte len „**incident**“) ihneď potom, ako sa o takejto udalosti dozvedia. Zmluvné strany sa zároveň zaväzujú spoločne vyvinúť maximálne úsilie na to, aby sa odstránili následky incidentu, aby sa zabránilo vzniku ďalších incidentov a zároveň, aby sa zabezpečili a obnovili všetky opatrenia potrebné na ochranu dôverných informácií v zmysle tejto Zmluvy.

Článok XII.
USTANOVENIA O KYBERNETICKEJ BEZPEČNOSTI

1. Objednávateľ je prevádzkovateľom základnej služby v zmysle zákona o kybernetickej bezpečnosti.

2. Objednávateľ vyhlasuje, že si je vedomý svojich zákonných povinností a prijal všetky potrebné bezpečnostné opatrenia stanovené príslušnými právnymi predpismi pre oblasť kybernetickej bezpečnosti, má zodpovedajúce materiálne, technické a personálne vybavenia a zaväzuje sa poskytnúť Zhotoviteľovi potrebnú súčinnosť a informácie, aby mohol efektívne napĺňať ustanovenia tejto Zmluvy.

3. Zhotoviteľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tohto článku Zmluvy a že disponuje technickým vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné pre zaistenie požiadaviek podľa tohto článku Zmluvy.

4. Zhotoviteľ je povinný prijímať a dodržiavať bezpečnostné opatrenia na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve a v príslušných právnych predpisoch tak, aby bol naplnený účel tejto Zmluvy.

5. Zhotoviteľ je povinný dodržiavať bezpečnostné požiadavky a opatrenia, ktoré sú kladené na tretie strany v zmysle § 10 zákona o kybernetickej bezpečnosti a vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej v texte len „**vyhláška NBÚ**“).

6. Zhotoviteľ je povinný dodržiavať a prijímať iba tie bezpečnostné opatrenia, ktoré je potrebné vykonať v súvislosti s realizáciou Diela, zohľadňujúc charakter a rozsah Predmetu plnenia.

7. Pre oblasť technických zraniteľností systémov a zariadení realizuje Zhotoviteľ opatrenia podľa § 9 vyhlášky NBÚ, najmä identifikuje technické zraniteľnosti informačných systémov a sietí prostredníctvom nasledovných opatrení:
   a) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí;
   b) zavedenie a prevádzka nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí;
   c) využitie verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

8. Pre oblasť riadenia bezpečnosti sietí a informačných systémov, realizuje Zhotoviteľ opatrenia podľa § 10 vyhlášky NBÚ, prostredníctvom nasledovných opatrení:
   a) riadenie bezpečného prístupu medzi vonkajšími a vnútornými sieťami a informačnými systémami Objednávateľa, a to najmä využitím nástrojov na ochranu integrity sietí a informačných systémov, ktoré sú zabezpečené segmentáciou sietí a informačných systémov; servery so službami priamo prístupnými z externých sietí sa nachádzajú v samostatných sieťových segmentoch a v rovnakom segmente musia byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom;

b) povoľovanie prepojenia medzi segmentmi a externými sieťami, ktoré sú chránené firewallom a všetkých spojení, na princípe zásady najnižších privilégií;
c) zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a informačného systému a vzdialený prístup, napríklad bezpečným spôsobom s použitím dvojfaktorovej autentizácie alebo použitím kryptografických prostriedkov;
d) sieťam alebo informačným systémom sú umožnené len špecifikované služby umiestnené vo vyhradených segmentoch počítačovej siete;
e) spojenia do externých sietí sú smerované cez sieťový firewall a v závislosti od prostredia aj cez systém detekcie prienikov;
f) servery dostupné z externých sietí sú zabezpečované podľa odporúčaní výrobcu;
g) udržiavanie zoznamu všetkých vstupno-výstupných bodov na hranici siete v aktuálnom stave;
h) zavedenie a prevádzka automatizačných prostriedkov, ktorými sú identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou;
i) blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie informačného systému umožňuje;
j) neumožnenie komunikácie a prevádzky aplikácií cez neautorizované porty;
k) zavedenie a prevádzka systému monitorovania bezpečnosti, ktorý je nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete;
l) implementácia systému detekcie prienikov alebo systému prevencie prienikov na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky;
m) smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu;
n) vyžadované použitie dvojfaktorovej autentizácie od každého vzdialeného pripojenia do siete Objednávateľa;
o) vykonávanie pravidelného alebo nepretržitého posudzovania technických zraniteľností, najmä identifikácie možnej prítomnosti škodlivého kódu zariadenia, ktoré sa vzdialene pripája do internej siete, alebo zmluvného zaručenia vrátane preukázania plnenia tejto povinnosti.

9. Pre oblasť riadenia prístupov realizuje Zhotoviteľ opatrenia podľa § 12 vyhlášky NBÚ, prostredníctvom nasledovných opatrení:
a) riadenie prístupov osôb k sieti a informačnému systému, založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému;
b) riadenie prístupov k sieťam a informačným systémom uskutočnené v závislosti od prevádzkových a bezpečnostných potrieb Prevádzkovateľa základnej služby, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a informačných systémov a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou;
c) riadenie prístupov osôb k sieti a informačnému systému, to zahŕňa najmenej vypracovanie zásad riadenia prístupu k informáciám; riadenia prístupu používateľov; zodpovednosti používateľov; riadenia prístupu k sieťam; prístupu k operačnému systému a jeho službám; prístupu k aplikáciám; monitorovania prístupu a používania informačného systému a riadenia vzdialeného prístupu;
d) pridelenie jednoznačného identifikátora na autentizáciu na vstup do siete a informačného systému každému používateľovi siete a informačného systému;
e) zabezpečenie riadenia jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov;
f) využitie nástroja na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom

ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy);

g) výkon kontroly prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov v pravidelných intervaloch;

h) určenie osoby zodpovednej za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému v zmysle príslušnej bezpečnostnej politiky.

10. Pre oblasť riešenia kybernetických bezpečnostných incidentov realizuje Zhotoviteľ opatrenia podľa § 14 vyhlášky NBÚ, najmä deteguje a rieši kybernetické bezpečnostné incidenty, ktoré môžu mať dopad na poskytovanie služieb Objednávateľa. To zahŕňa najmä prijatie nasledovných opatrení:

a) monitorovanie a analyzovanie udalostí v sieťach a informačných systémoch, ktoré sú využívané na poskytovanie služieb Objednávateľa;

b) detegovanie kybernetických bezpečnostných incidentov, prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát;

c) zber a vyhodnocovanie relevantných informácií o kybernetických bezpečnostných incidentoch prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch; vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetický bezpečnostným incidentom; vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako kybernetických bezpečnostných incidentov; revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch;

d) riešenie zistených kybernetických bezpečnostných incidentov a zníženie následkov zistených kybernetických bezpečnostných incidentov podľa pokynov Objednávateľa;

e) vyhodnocovanie spôsobov riešenia kybernetických bezpečnostných incidentov po ich vyriešení a prijatie opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných kybernetických bezpečnostných incidentov v súčinnosti s Objednávateľom.

11. Pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov realizuje Zhotoviteľ opatrenia podľa § 15 vyhlášky NBÚ, najmä zaznamenáva činnosti sietí a informačných systémov a ich používateľov najmenej pre všetky informačné systémy a sieťové prvky, ktoré sú priamo využívané pri poskytovaní služieb Objednávateľa.

12. Zhotoviteľ sa zaväzuje na plnenie tejto Zmluvy a bezpečnostných opatrení postupovať v súlade so schválenými normami upravujúcimi oblasť informačnej bezpečnosti a to najmä podľa STN ISO/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti) a vyhláškou NBÚ.

13. Zhotoviteľ je povinný bezodkladne hlásiť a informovať Objednávateľa o každom svojom podozrení na kybernetický bezpečnostný incident, ako aj o všetkých skutočnostiach majúcich negatívny vplyv na zabezpečovanie kybernetickej bezpečnosti prevádzkovanej základnej služby, a to prostredníctvom elektronickej pošty na kontaktné adresy Objednávateľa uvedené v záhlaví tejto Zmluvy.

14. Hlásenie podozrenia o kybernetickom bezpečnostnom incidente musí obsahovať najmä informácie:

a) tom, kto hlási kybernetický bezpečnostný incident, a to identifikačné údaje a kontaktné údaje;
b) o kybernetickom bezpečnostnom incidente, a to časové údaje priebehu kybernetického bezpečnostného incidentu, opis priebehu kybernetického bezpečnostného incidentu a rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu;
c) o službe zasiahnutej kybernetickým bezpečnostným incidentom, a to konkrétny popis všetkých zasiahnutých aktív a vplyv kybernetického bezpečnostného incidentu na poskytovanú službu;
d) o riešení kybernetického bezpečnostného incidentu, a to stav riešenia kybernetického bezpečnostného incidentu, vykonané nápravné opatrenia a popis následkov kybernetického bezpečnostného incidentu.

15. Pri riešení kybernetických bezpečnostných incidentov je Zhotoviteľ povinný spolupracovať s Objednávateľom, Národným bezpečnostným úradom a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získane z vlastnej činnosti podľa tejto Zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického bezpečnostného incidentu.

16. Zhotoviteľ je povinný v čase kybernetického bezpečnostného incidentu v rozsahu jeho oprávnení zabezpečiť dôkazy, ktoré budú slúžiť na objasnenie vzniku a riešenia kybernetického bezpečnostného incidentu.

17. Objednávateľ je povinný informovať v nevyhnutnom rozsahu Zhotoviteľa o kybernetickom bezpečnostnom incidente, o ktorom sa dozvedel ako prvý, a ktorý môže mať vplyv na plnenie tejto Zmluvy.

18. Zmluvné strany vyhlasujú, že ustanovenia tejto zmluvy nezbavujú Zmluvné strany zodpovednosti za plnenie vlastných povinností, ktoré im vyplývajú z právnych predpisov na úseku kybernetickej bezpečnosti.

19. Ustanovenia tohto článku Zmluvy sa Zhotoviteľ zaväzuje dodržiavať minimálne počas celej doby platnosti Zmluvy ako aj počas trvania záručnej doby špecifikovanej v článku VII. bod 3. Zmluvy, pokiaľ z právnych predpisov nevyplývajú určité povinnosti pre Zhotoviteľa aj po skončení tejto doby.

20. Zmluvné strany sa výslovne dohodli, že cena za poskytnutie všetkých bezpečnostných opatrení a notifikačných povinností podľa tohto článku Zmluvy je zahrnutá v Cene za Dielo bližšie špecifikovanej v článku V. bod 2. Zmluvy. V prípade vzniku nákladov na strane Zhotoviteľa v súvislosti s plnením povinností podľa tohto článku Zmluvy, tieto znáša Zhotoviteľ.

21. Zhotoviteľ berie na vedomie, že neplnenie jeho povinností v zmysle tohto článku Zmluvy môže spôsobiť Objednávateľovi škody, pričom v prípade škôd ako dôsledkov kybernetických bezpečnostných incidentov, ktoré by sa pri riadnom a včasnom plnení povinností Zhotoviteľa neprejavili alebo by sa prejavili v menšej intenzite, zodpovedá Objednávateľovi v plnom rozsahu.

Článok XIII.
ZÁVERČNÉ USTANOVENIA

1. Predmetná zmluva je vyhotovená v piatich (5) vyhotoveniach, z ktorých každé má charakter originálu, štyri (4) vyhotovenia obdrží Objednávateľ a jedno (1) jej vyhotovenie obdrží Zhotoviteľ.

2. Zmluvné strany si dohodli ako podmienku platnosti tejto zmluvy, ako aj jej prípadných dodatkov, písomnú formu a dohodu v celom rozsahu.

3. Pre prípad, že po dobu trvania tohto zmluvného vzťahu dôjde k akejkoľvek zmene v identifikačných údajoch Zmluvných strán uvedených v záhlaví tejto Zmluvy, každá zo zmluvných strán je povinná oznámiť takúto zmenu druhej Zmluvnej strane, a to bezodkladne po tom, ako k takej zmene dôjde, ibaže by táto zmena bola zrejmá z verejného registra, kde je príslušná Zmluvná strana zapísaná.

4. Zmluvné strany sa zaväzujú riešiť spory prednostne formou uzatvorenia zmieru. V prípade, že sa spor nevyrieši uzatvorením zmieru, zmluvné strany sú oprávnené predložiť spor na riešenie príslušnému súdu v Slovenskej republike.

5. Zmluvné strany vyhlasujú, že im nie sú známe žiadne okolnosti, ktoré by bránili platne uzavrieť túto Zmluvu. V prípade, že taká okolnosť existuje, zodpovedajú za škodu, ktorá tým druhej Zmluvnej strane vznikne.

6. Zmluvné strany zároveň vyhlasujú, že si text Zmluvy riadne prečítali, jeho obsahu porozumeli, sú si vedomé všetkých právnych následkov vyplývajúcich z tejto Zmluvy, Zmluva vyjadruje ich slobodnú a vážnu vôľu bez akýchkoľvek omylov, čo potvrdzujú vlastnoručnými podpismi.

7. Na právne vzťahy osobitne neupravené touto Zmluvou sa vzťahujú príslušné ustanovenia Obchodného zákonníka, príp. ustanovenia ostatných právnych predpisov platných v Slovenskej republike.

8. Neoddeliteľnú súčasť tejto Zmluvy tvoria nasledovné prílohy:
   - Príloha č. 1: Projektový zámer, Prístup k projektu a Funkčná špecifikácia;
   - Príloha č. 2: Zoznam odborných kapacít Zhotoviteľa;
   - Príloha č. 3: Zoznam subdodávateľov;
   - Príloha č. 4: Rozpočet (Súťažná cenová ponuka Zhotoviteľa

V Banskej Bystrici, dňa: .....

V Bratislave, dňa: .....

Za Objednávateľa:

Za Zhotoviteľa:

Ján Nosko
primátor Mesta Banská Bystrica

Ing. Peter Máčaj
predseda predstavenstva
Slovanet, a.s.

Ing. Peter Tomášek
člen predstavenstva
Slovanet, a.s.

Príloha č.1 Zmluvy

Projektový zámer, Prístup k projektu a Funkčná špecifikácia

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

PROJEKTOVÝ ZÁMER

Vzor pre manažérsky výstup I-02

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	Mesto Banská Bystrica
Názov projektu	Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica
Zodpovedná osoba za projekt	Ing. Beáta Galková
Realizátor projektu	Mesto Banská Bystrica
Vlastník projektu	Ing. Bibiána Palušková

Schvaľovanie dokumentu

Položka	Meno a priezvisko	Organizácia	Pracovná pozícia	Dátum	Podpis (alebo elektronický súhlas)
Vypracoval	Ing. Bibiána Palušková	Mesto Banská Bystrica	Manažér kybernetickej bezpečnosti	20.04.2024	

Obsah

1. HISTÓRIA DOKUMENTU

Verzia	Dátum	Zmeny	Meno
0.1	03.04.2024	Draft pracovnej verzie	Ing. Bibiána Palušková
0.2	20.04.2024	Zapracované pripomienky z v 0.1	Ing. Bibiána Palušková
1.0	26.4.2024	Predložené na schválenie	Ing. Bibiána Palušková
1.1	14.1.2025	Oprava názvu položky pre switch typ 1 a typ 2 (stakovacia šírka pásma)	Ing. Bibiána Palušková

2. ÚČEL DOKUMENTU, SKRATKY (KONVENCIE) A DEFINÍCIE

V súlade s **Vyhláškou Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy** je dokument I-02 Projektový zámer určený na rozpracovanie podrobných podporných informácií prípravy projektu, aby bolo možné rozhodnúť o pokračovaní prípravy, projektu, pláne realizácie, alokovaní rozpočtu a ľudských zdrojov.

Dokument Projektový zámer v zmysle vyššie uvedenej vyhlášky obsahuje manažérske zhrnutie, rozsah, ciele a motiváciu Povinnej osoby (ďalej len Mesto alebo Mesto Banská Bystrica alebo Objednávateľ) realizovať projekt. Dokument zároveň uvádza informácie o zainteresovaných stranách, prístup k známym alternatívam smerovania a riadenia projektu, návrh merateľných ukazovateľov s ohľadom na schému uvažovaného financovania, podrobný popis požadovaných projektových výstupov ako aj obmedzení projektu, projektový predpokladov a tolerancií ako aj návrh organizačného zabezpečenia projektu.

Súčasťou predkladaného Projektového zámeru je detailný opis rozpočtu projektu a prínosov projektu v kontexte odhadovaných projektových nákladov, náhľad relevantných domén architektúr, ak ich realizácia projektu ovplyvňuje ich zmenu ako aj plánovaný časový harmonogram projektu s väzbami na plánované aktivity a výstupy projektu v súlade s konvenciou riadenia projektov PRINCE2.

2.1 Použité skratky a pojmy

SKRATKA	POPIS
TBD	To Be Determined (ešte určiť)
IB	Informačná bezpečnosť
KB	Kybernetická bezpečnosť
ITVS	Informačné technológie a výpočtové systémy
IKT	Informačné a komunikačné technológie
AR/BIA	Analýza rizík/Business Impact Analysis
HW	Hardvér (hardware)
SW	Softvér (software)
IS	Informačný systém
BCM	Business Continuity Management
DRP	Disaster Recovery Plan
OTP	One-Time Password
IT	Informačné technológie
IEEE 802.1X	Štandard pre kontrolu prístupu do siete
CAPEX	Kapitálové výdavky (Capital Expenditure)
OPEX	Prevádzkové výdavky (Operating Expenditure)

2.2 Konvencie pre typy požiadaviek (príklady)

Užívateľské požiadavky majú nasledovnú konvenciu:

U_nn_Rxx

- U – užívateľská požiadavka
- Nn – typ používateľa
- R – označenie požiadavky
- Xx – číslo požiadavky

Procesné požiadavky majú nasledovnú konvenciu:

P_ABXY_Rxx

- P - procesná požiadavka
- AB – označenie procesu
- XY – číslo podprocesu
- R – označenie požiadavky
- Xx – číslo požiadavky

Požiadavky na reporting majú nasledovnú konvenciu:

R_ABXY_Rxx

- R – požiadavka na reporting
- Nn – číslo reportu
- R – označenie požiadavky
- Xx – číslo požiadavky

3. DEFINOVANIE PROJEKTU

3.1 Manažérske zhrnutie

Jedným zo strategických cieľov Koncepcie kybernetickej bezpečnosti schválenej v roku 2015 vládou Slovenskej republiky je otvorený, bezpečný a chránený kybernetický priestor, ktorý zabezpečí vybudovanie dôvery v spoľahlivosť a bezpečnosť štátu a to najmä kritickej infraštruktúry a komunikačnej infraštruktúry, ako aj istoty, že tieto budú plniť svoje funkcie a slúžiť národným záujmom. Na druhej strane situácia v oblasti informačnej a kybernetickej bezpečnosti vo verenej správe nie je v ideálnom stave a kondícii. Väčšina orgánov verejnej správy nemá implementované riešenia a opatrenia kybernetickej bezpečnosti povinné podľa zákona o KB a zákona o ITVS. Z externého pohľadu sa zvyšuje frekvencia a závažnosť útokov z externého prostredia a na druhej strane sa zvyšuje závislosť orgánov verejnej správy na informačných aktívach a informačných systémoch, na ktorých je činnosť orgánov verejnej správy neodbytne závislá. Zvyšujú sa teda hrozby, zraniteľnosti a následne aj možné dopady bezpečnostných incidentov. Projektový zámer vychádza z horeuvedenej koncepcie ako aj strategických cieľov **Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025**[1], ktorá definuje strategické ciele Slovenskej republiky v oblasti kybernetickej a informačnej bezpečnosti. Tento strategický dokument v bode 4.4 definuje kybernetickú bezpečnosť (ďalej ako „KB") ako základnú súčasť verejnej správy: ***„V kybernetickom priestore musia dobre fungovať nielen služby súkromných spoločností, ale aj tie poskytované štátom".*** *Služby, ktoré ponúka svojim občanom musia byť dostatočne zabezpečené, aby nedošlo k zneužitiu citlivých alebo osobných údajov v kontexte Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679".* Mesto Banská Bystrica ako Povinná osoba a iniciátor tohto projektového zámeru si plne uvedomuje, že súčasné kybernetické hrozby v kontexte svetových udalostí nie sú len hrozbami fiktívnymi, ale predstavujú skutočné riziko, ktoré ohrozuje informačné aktíva v jeho gescii a prevádzke ako prevádzkovateľa základnej služby. Mesto Banská Bystrica má v oblasti IKT dlhodobo víziu napĺňať ciele Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025, ako aj zodpovedne pristupovať k zabezpečeniu a riadeniu svojich informačných aktív prostredníctvom uplatňovania systematického prístupu ku kybernetickej a informačnej bezpečnosti založenej na analýze a riadení rizík, prostredníctvom poskytovania bezpečných a dostupných elektronických služieb mesta ako subjektu verejnej správy pre všetkých svojich občanov, podnikateľov ako aj návštevníkov. **Motiváciou Mesta Banská Bystrica predložiť tento projektový zámer a realizovať projekt je reflektovať na známe zistenia z už vykonaných auditov KB realizovaných v jeho prostredí, tak, aby projekt v čo najväčšej miere prispel k zosúladeniu oblasti riadenia kybernetickej a informačnej bezpečnosti s požiadavkami a očakávaniami príslušných štátnych orgánov ako aj príslušných aktuálne platných legislatívnych požiadaviek.** Mesto Banská Bystrica sa napriek identifikovaným viacerým potrebným opatreniam v oblasti zabezpečenia informačnej a kybernetickej bezpečnosti rozhodlo pre zameranie sa na opatrenia, ktoré predstavujú najvyššiu mieru rizika a najvyššie možné dopady v kontexte súčasne identifikovaného nesúladu s legislatívnymi požiadavkami, ktoré vyplývajú z ostatne vykonaného auditu kybernetickej bezpečnosti. Rozsah projektového zámeru súčasne vychádza z vykonanej viacfaktorovej analýzy možných alternatív ako variantných riešení a teda navrhované riešenie ako optimálne je vytvorené na základe predošlej uskutočnenej dôslednej selekcie.

Mesto Banská Bystrica si uvedomuje, že vývoj v oblasti informačných a komunikačných technológií, narastajúca komplexnosť, diferencovanosť, technologická rozmanitosť súčasne zvyšujú rozsah perimetra pre vykonanie kybernetického útoku, ktorých prípadné vykonanie by ohrozilo riziko dôvery Mesta Banská Bystrica u používateľov poskytovanej základnej služby. Z tohto dôvodu Mesto Banská Bystrica považuje za nevyhnutné prijímať a realizovať opatrenia na ochranu svojich informačných aktív vrátane zabezpečenia informácií, ktoré sú vo veľkej miere v rámci implementácie efektívnej verejnej správy (teda aj v oblasti miestnej samosprávy) poskytované, ukladané

[1] https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Narodna-strategia-kybernetickej-bezpecnosti.pdf

a vymieňané v kybernetickom priestore. Zavedením správnych opatrení je možné minimalizovať riziká, ktoré kybernetický priestor pre Mesto Banská Bystrica prináša a to hlavne:

- Odcudzenie, zneužitie alebo strata dôvernosti a/alebo dostupnosti osobných a inak citlivých údajov;
- Poškodenie reputácie Mesta Banská Bystrica ako poskytovateľa základnej služby a služieb pre občanov;
- Znefunkčnenie poskytovaných elektronických služieb pre občanov mesta.

Mesto Banská Bystrica definuje tento Projektový zámer nie len s ohľadom na prístup štátu v oblasti zabezpečenia informačnej a kybernetickej bezpečnosti, ale aj s ohľadom na vlastné potreby, ktoré boli identifikované na základe zistení a odporúčaní ostatne vykonaného auditu kybernetickej a informačnej bezpečnosti, ktorý bol vykonaný v súlade s § 29 Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej „Zákon o KB")[2]. V súlade s § 20 Zákona o KB je Mesto Banská Bystrica povinné plniť predmetné opatrenia, ktorými bude zabezpečovať pokrytie významných aspektov kybernetickej bezpečnosti, ktoré majú vplyv na celú organizáciu. **Cieľom projektu je zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.** Vzhľadom na šírku oblastí bezpečnostných opatrení ako aj na technické, administratívne a finančné kapacity Mesta Banská Bystrica boli ciele projektu identifikované s dôrazom na ich čo najväčší efekt a predpokladaný pozitívny dopad na oblasť informačnej a kybernetickej bezpečnosti organizácie, ktorá je prevádzkovateľom základnej služby. K prioritizácii riešených oblastí Mesto Banská Bystrica dospelo na základe ostatne vykonaného auditu kybernetickej a informačnej bezpečnosti ako aj potreby vykonania opakovaného auditu informačnej a kybernetickej bezpečnosti. V rámci projektu má Mesto Banská Bystrica zámer realizovať nasledovné opatrenia na zvýšenie úrovne informačnej a kybernetickej bezpečnosti, ktoré prispejú k celkovému zlepšeniu technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti kybernetickej a informačnej bezpečnosti v jeho prostredí:

1. Vykonať opakovaný audit informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB;
2. Vypracovať relevantnú bezpečnostnú dokumentáciu;
3. Implementovať a konfigurovať systém pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica;
4. Vykonať segmentáciu siete Mesta Banská Bystrica s ohľadom na súčasné prevádzkové požiadavky;
5. Zrealizovať výmenu aktívnych prvkov core časti siete;
6. Implementovať systém dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete;
7. Implementovať riešenie centrálneho bezpečnostného manažmentu pre koncové stanice;

V rámci jednotlivých aktivít Mesto plánuje vykonať školenie dotknutého personálu na implementované technológie a riešenia, tak aby bola zabezpečená kontinuita business procesov ako aj udržateľnosť projektu 60 kalendárnych mesiacov po ukončení jeho realizačnej fázy.

Motívom realizácie horeuvedených opatrení sú okrem uvedeného aj nasledovné dôvody:

- Potreba odbúravania agendy a odľahčenie nedostatočných personálnych kapacít pre oblasť riadenia IB a KB na prevádzku bezpečnostných systémov;
- Absencia realizácie základnej analýzy rizík a analýzy dopadov (AR/BIA);
- Absencia uceleného konceptu riadenia rizík a absencia spracovania základných dokumentov v oblasti KB a IB a akvizície HW a SW komponentov v súlade so Zákonom o KB.

Realizácia vyššie uvedených opatrení prispeje k celkovému zvýšeniu úrovne informačnej bezpečnosti a kybernetickej bezpečnosti ako aj k odstraňovaniu zistení a nesúladov identifikovaných v ostatne vykonanom audite kybernetickej a informačnej bezpečnosti, čo jednoznačným spôsobom reflektuje zámer Mesta Banská Bystrica alokovať svoje zdroje a kapacity na oblasti informačnej a kybernetickej bezpečnosti, v rámci ktorých sú objektívne identifikované najvyššie miery rizika, potenciálny dopad a najvyššia miera nesúladu s legislatívnymi požiadavkami.

Iniciatíva projektu a zdôvodnenie projekt realizovať zároveň vychádza z viacerých vzájomne previazaných predpokladov a potrieb:

- Nárast rizika kybernetických útokov zameraných na subjekty verejnej správy a prevádzkovateľov základnej služby;
- Potreba zvýšenia efektivity procesov riadenia informačnej a kybernetickej bezpečnosti rámci IKT organizácie;
- Potreba riešenia nedostatku kvalifikovaných odborných IKT špecialistov a špecialistov informačnej bezpečnosti a kybernetickej bezpečnosti prostredníctvom centrálnej správy, automatizácie a manažmentu procesov a aktív;
- Potreba zvýšenia transparentnosti a efektívnosti manažmentu výkonu prevádzky IKT v organizácii;
- Potreba zvýšenia visibility v monitorovaných IS prostredníctvom implementácie manažmentových a dohľadových nástrojov;
- Naplnenie zákonných a regulatívnych požiadaviek;
- Zvýšiť bezpečnosť siete prostredníctvom rozšírenia prístupových pravidiel pri zachovaní užívateľského komfortu;
- Absencia vykonania inventarizácie informačných aktív, vykonania klasifikácie a kategorizácie IS a sietí, vykonania AR a BIA ako aj absencia zabezpečenia formalizovaného a opakovaného procesu riadenia identifikovaných rizík (ich mitigácie), ktoré sú nevyhnutným a nutným predpokladom pre efektívne riadenie rizík IB a KB;
- Absencia bezpečnostných opatrení pre jednotlivé klasifikačné stupne a kategórie IS a absencia základnej sady dokumentácie požadovanej Zákonom o KB;
- Absencia základných smerníc pre výkon procesov riadenia IB a KB v rámci jednotlivých oblastí riadenia;
- Absencia ľudských kapacít na efektívny bezpečnostný monitoring, konsolidáciu logov a auditných záznamov, analýzu bezpečnostných udalostí a incidentov a aj na ich riešenie so súčasnou snahou odbúrania pracovnej záťaže prechodom na automatizáciu a digitalizáciu týchto procesov.

Navrhované opatrenia predstavujú vzhľadom na aktuálny stav IB a KB Mesta Banská Bystrica nutný základ pre zefektívnenie riadenia IB a KB ako aj základ pre implementáciu dodatočných opatrení a technických bezpečnostných riešení. Výstupy týchto opatrení možno vnímať ako nevyhnutný predpoklad pre prijímanie adekvátnych, efektívnych, vyvážených a optimálnych bezpečnostných opatrení. Mesto Banská Bystrica realizáciou projektu zároveň očakáva, že okrem samotného zvýšenia úrovne IB a KB vytvorí dostatočný základ v oblasti governance ako aj v oblasti technických opatrení, ktorý mu umožní aj v budúcnosti nadväzovať na aktivity tohto projektu tak, aby mesto mohlo získavať opakovane externé zdroje pre kontinuálny a koncepčný rozvoj v oblasti IB a KB, nakoľko túto situáciu

[2] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/

nevníma ako statickú entitu ale ako dynamický, neustále sa rozvíjajúci a živý proces, ktorý odráža zaužívané princípy efektívneho riadenia IKT aktív so zameraním sa na kontinuálne zlepšovanie.

Realizácia horeuvedených opatrení bude zároveň podporená školeniami dotknutých stakeholderov tak, aby prechod na novo implementované riešenia a obstarané HW a SW komponenty bol plynulý a bola zabezpečená kontinuita prevádzky služieb poskytovaných pred realizáciou projektu. Ciele projektu korešpondujú s víziou Mesta Banská Bystrica byť **odolným, inovatívnym a inteligentným, bezpečným mestom**[3], a teda rozvíjať bezpečnosť vo všetkých oblastiach života mesta vrátane informačnej a kybernetickej bezpečnosti (súlad s navrhovaným špecifickým cieľom **8.1.2 Rozvíjať bezpečnosť vo všetkých oblastiach života mesta.**

Očakávané prínosy projektu:

- Aktualizácia overenia plnenia povinností podľa Zákona o KB spolu s posúdením zhody prijatých bezpečnostných opatrení s požiadavkami podľa Zákona o KB, ktoré sa vzťahujú na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby;
- Preverenie účinnosti doposiaľ prijatých bezpečnostných opatrení a odpočet plnenia požiadaviek stanovených Zákonom o KB;
- Zavedenie systému pre zabezpečenie siete a správu identít a zabezpečenie prístupov do siete a k aktívam v sieti;
- Zvýšenie úrovne zabezpečenia siete, jej výkonnosti, správy ako aj ochrany vykonaním segmentácie siete;
- Zvýšenie úrovne a rozsahu centralizovanej správy a sledovania siete, rozšírenie rozsahu nástrojov na diagnostiku a analýzu a zabezpečenie pokročilejších bezpečnostných funkcií prostredníctvom výmeny zastaralých, end-of-support a end-of-sales aktívnych sieťových prvkov;
- Zvýšenie bezpečnosti pri prístupe k aktívam, zníženie rizika zneužitia hesiel, zvýšenie ochrany citlivých údajov a dodatočné zvýšenie úrovne zabezpečenia prístupu do siete zavedením dvojfaktorovej autentifikácie.

Podrobnejší opis opatrení (aktivít projektu):

Všetky aktivity projektu má Mesto Banská Bystrica záujem financovať prostredníctvom kombinácie zdrojov EÚ, národných zdrojov a vlastných zdrojov v rámci aktuálne vyhlásenej Výzvy „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejná správa", kód výzvy PSK-MIRRI-611-2024-DV-EFRR, (ďalej len „Výzva") v súlade s možnou mierou intenzity spolufinancovania uvedenou v časti 4 Výzvy. V prípade nezískania prostriedkov, nebude možné pristúpiť k realizácii optimálneho variantného riešenia.

1. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB

Zámerom tejto aktivity je vykonanie pravidelne opakujúceho sa auditu IB a KB v súlade s § 29 Zákona o KB. Mesto Banská Bystrica v čase kreovania tohto projektového zámeru má plán realizovať audit s už jestvujúcim zmluvným partnerom. Vzhľadom na skutočnosť, že zahájenie opakovaného auditu pripadá na obdobie, ktoré časovo pripadá dátumu po vyhlásení Výzvy, Mesto Banská Bystrica má v pláne využiť možnosť financovať náklady vzniknuté po tomto období, čo rozsahovo zodpovedá celému auditu, ktorý sa plánuje realizovať. Aktivita bude pozostávať z preplatenia nákladov spojených s činnosťou špecialistov z oblasti IB a KB podieľajúcich sa na výkone opakovaného auditu. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy" a „Harmonogram jednotlivých fáz a metóda jeho riadenia".

Väzba na oprávnenú aktivitu z Výzvy: O.2) Audit a kontrolné činnosti – Obstaranie prvého alebo opakovaného auditu kybernetickej bezpečnosti v súlade so zákonom o KB.

2. Vypracovanie relevantnej bezpečnostnej dokumentácie

Mesto Banská Bystrica momentálne nedisponuje žiadnou z povinnej dokumentácie v zmysle Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných opatrení v znení vyhlášky č. 264/2023 Z. z. Z tohto dôvodu je jednou z hlavných priorít v rámci uvažovaného projektu zabezpečiť dopracovanie relevantnej dokumentácie a zosúladenie so zákonnými požiadavkami kladenými na poskytovateľa základnej služby. V súčasnosti Mesto Banská Bystrica disponuje iba zriadeným bezpečnostným výborom, ale samotné riadenie IB a KB nie je formalizované. Predmetom tejto aktivity sú nasledovné činnosti a vypracovanie nasledovnej bezpečnostnej dokumentácie zohľadňujúcej aktuálny stav a potreby Mesta:

- Vykonanie inventarizácie aktív vrátane klasifikácie informácií a kategorizácie sietí a informačných systémov;
- Vypracovanie analýzy rizík (AR) podľa požiadaviek uvedených v Zákone o KB;
- Vypracovanie analýzy dopadov a kľúčových procesov a činností (BIA) vrátane prípravy smernice/metodiky pre riadenie oblasti BCM, prípravy plánov BCM a plánov obnovy DRP.
- Vypracovanie základných bezpečnostných politík KB:
    - Bezpečnostná stratégia kybernetickej bezpečnosti;
    - Politika organizácie bezpečnosti;
    - Politika pre riadenie bezpečnosti rizík;
    - Politika pre riadenie informačných aktív;
    - Pravidlá správania a dobrej praxe;
    - Politika pre riadenie dodávateľských vzťahov;
    - Politika pre riadenie vývoja a údržby v oblasti IKT;
    - Politika pre riadenie a prevádzku IKT;
    - Politika pre riadenie súladu;
    - Politika pre riadenie kontinuity procesov a činností.

Aktivita bude pozostávať z poskytnutia služieb – činností expertov v oblasti IB a KB. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy" a „Harmonogram jednotlivých fáz a metóda jeho riadenia".

Väzba na oprávnené aktivity z Výzvy: A.1) Organizácia KIB – Vypracovanie alebo aktualizácia bezpečnostnej dokumentácie vrátane rozsahu a spôsobu plnenia všeobecných bezpečnostných opatrení.

[3] https://tvormespolu.banskabystrica.sk/processes/programrozvojamesta

3. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica

Mesto Banská Bystrica momentálne rieši prístup do siete iba na úrovni prihlasovacie meno + heslo v rámci užívateľov vytvorených v rámci Active Directory. V súčasnom stave je možné sa však v rámci vnútornej siete pripojiť prostredníctvom akéhokoľvek zariadenia, keďže nejestvujú žiadne politiky a nástroje, ktoré by umožňovali definovať rozsah/typy/skupiny zariadení, ktorých prístup do siete je povolený.

Táto situácia predstavuje značné riziko vzniku kybernetického incidentu, keďže prevádzka a správa IKT Mesta nemá možnosti a nástroje ako takýmto prístupom efektívne zabrániť. Zámerom v rámci tejto aktivity je obstarať a nasadiť SW riešenie, pomocou ktorého bude možné vykonávať centralizovanú autentifikáciu a autorizáciu pre rôzne typy používateľov a zariadení v sieti, spravovať politiky prístupu na základe definovania identít, rolí, zariadení, prípadne ďalších správcom siete voliteľných atribútov, sledovať a revidovať prístupy používateľov do siete, spravovať prístupy do siete zariadeniami pristupujúcimi v režime BYOD („Bring Your Own Device") – zariadení, ktoré nie sú v správe a priamej kontrole správcu IKT Mesta. Implementácia takéhoto riešenia zjednotí, zjednoduší a urýchli správu prístupov v rámci siete Mesta Banská Bystrica. Nasadené riešenie bude súčasne podporovať štandard IEEE 802.1X pre autentifikáciu a autorizáciu zariadení, ktoré budú nadväzovať spojenie so sieťou Mesta. Riešenie bude zabezpečovať kontrolu prístupu do siete na úrovni portov na aktívnych sieťových prvkoch. Pre účely plnohodnotného nasadenia overovania na úrovni celej siete organizácie bude potrebné realizovať výmenu sieťových prvkov, ktoré sú „end-of-sales" a „end-of-support" a súčasne nepodporujú protokol 802.1X. Z tohto dôvodu je zámerom Mesta Banská Bystrica realizovať nákup nových aktívnych sieťových prvkov, ktoré budú súčasťou implementovaného riešenia v celkovom počte 7 ks.

Aktivita bude pozostávať z obstarania SW riešenia pre centrálnu správu prístupov / identít ako aj obstarania HW komponentov, ktoré podporujú protokol IEEE 802.1X. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy" a „Harmonogram jednotlivých fáz a metóda jeho riadenia".

Väzba na oprávnené aktivity z Výzvy: D.2) Riadenie prístupov – Zavedenie, implementácia alebo aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane prístupových práv a kontroly prístupových účtov a prístupových oprávnení.

4. Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky

Potreba realizácie segmentácie siete úzko súvisí s aktivitou č.3, nakoľko výstupy aktivity č.3 bude súčasne nevyhnutne potrebné koordinovať v kontexte logického členenia siete na segmenty zohľadňujúce prevádzkové a bezpečnostné požiadavky mesta. V súčasnosti Mesto Banská Bystrica nemá vykonanú komplexnú segmentáciu siete. V rámci projektu sa plánuje vykonať segmentácia siete súčasne s implementáciou a nasadením overovania podľa protokolu 802.1X. Realizácia segmentácie siete na logické celky v závislosti od súčasnej prevádzky, typov podsietí ako aj pristupujúcich používateľov a zariadení umožní rozdeliť sieť na VLAN, kde bude súčasne aplikovaná politika prístupov 802.1X, čo umožní lepšiu kontrolu prístupu na úrovni jednotlivých segmentov a to tak, že zariadenia bude možné pripojiť iba k segmentom, ktoré budú pre ne určené na základe ich identít a udelených prístupových práv/prístupových profilov. Kombináciou overovania prostredníctvom 802.1X a vykonaním segmentácie siete sa očakáva zvýšenie celkovej bezpečnosti siete, nakoľko možnosť použitia autentifikácie na každom segmente zabezpečí, že budú mať oprávnené zariadenia prístup iba do určitej časti siete, čo bude značným spôsobom minimalizovať riziko neoprávneného prístupu alebo pohybu zariadení v sieti. Implementáciou overovania 802.1X v kombinácií s vykonanou segmentáciou siete sa zároveň zabezpečí, že prípadné bezpečnostné incidenty a hrozby budú izolované na konkrétne menšie segmenty siete a identifikované problémové zariadenie nebude mať dopad na celú sieť ale len na konkrétny segment. Takéto nasadenie zároveň umožní dynamickú autentifikáciu zariadení a prístupov z pohľadu administrátora, ktorý bude môcť meniť prístupové pravidlá na úrovni portu ktoréhokoľvek segmentu.

Aktivita bude pozostávať z obstarania služieb činností expertov na sieťové a bezpečnostné technológie, ktorí vykonajú analýzu súčasného stavu, navrhnú optimálny budúci stav a zaistia vykonanie samotnej segmentácie siete v kontexte implementovaného overovania podľa 802.1X a obstaraných ako aj jestvujúcich aktívnych prvkov siete.

Väzba na oprávnené aktivity z Výzvy: I.1) Sieťová a komunikačná bezpečnosť – Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečnostného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel.

5. Výmena aktívnych prvkov CORE časti siete

Vzhľadom na skutočnosť, že podstatná časť CORE siete Mesta Banská Bystrica pozostáva z prevádzkovaných end-of-sale a end-of-support zariadení a zároveň sa neustále navyšujú potreby zvyšovania prenosovej rýchlosti a kapacity siete, Mesto Banská Bystrica potrebuje zabezpečiť výmenu vybraných aktívnych sieťových prvkov CORE časti siete, tak aby bola kontinuálne zachovaná vysoká úroveň bezpečnosti prevádzky siete prostredníctvom zachovania aktuálnych bezpečnostných funkcií zariadení aj vo vzťahu k aktuálne známym zraniteľnostiam a hrozbám od čoho sa očakáva zvýšenie celkovej úrovne zabezpečenia ochrany siete proti rôznym typom útokov. Vzhľadom na narastajúci počet aplikácií a systémov, ktoré Mesto Banská Bystrica spravuje, ako aj počet generovaných eventov v siete resp. requestov voči aplikáciám, ku ktorým pristupujú interní používatelia ako aj externí používatelia je potrebné zachovať vysokú úroveň dostupnosti všetkých prevádzkovaných IS Mesta. Výmenou potrebných aktívnych prvkov CORE časti siete Mesto Banská Bystrica zabezpečí kontinuálne požadovanú úroveň dostupnosti IT aktív a ich primeranú dobu odozvy. Výmena aktívnych prvkov v CORE časti siete je nevyhnutne potrebná aj vzhľadom na zámer vykonať segmentáciu siete Mesta ako aj implementovať systém pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica prostredníctvom protokolu IEEE 802.1X. Súčasný set dostupných sieťových prvkov neumožňuje plnohodnotné nasadenie tohto bezpečnostného protokolu, čo v praxi znamená, že by nebolo možné v rámci realizácie vyššie uvedených aktivít vykonať túto implementáciu cez všetky dotknuté oddelenia v sieti mestského úradu, na úrovni všetkých novo definovaných sieťových segmentov, čo by v podstate malo za následok, že efekt implementácie IEEE 802.1X s vykonaním segmentácie by mal len minimálny pozitívny dopad na organizáciu ako celok.

Aktivita bude pozostávať z obstarania aktívnych prvkov pre CORE časť siete, ktoré budú funkčne a výkonnostne zodpovedať požiadavkám na „TO-BE" stav nie len z ohľadom na celkový performance siete, ale aj s ohľadom na vysoké štandardy bezpečnosti siete.

Celkovo sa očakáva obstaranie 9 ks aktívnych prvkov pre CORE časť siete súčasne s vykonaním revízie konfigurácie a implementácie nových konfiguračných pravidiel vrátane pravidiel na firewalloch. Indikatívna výška prostriedkov ako aj časový horizont realizácie tejto aktivity sú uvedené v časti „Rozpočet a prínosy" a „Harmonogram jednotlivých fáz a metóda jeho riadenia".

Väzba na oprávnené aktivity z Výzvy: Väzba na oprávnené aktivity z Výzvy: D.2) Riadenie prístupov – Zavedenie, implementácia alebo aktualizácia centrálneho nástroja na správu a overovanie identity, nástroja na riadenie prístupových oprávnení vrátane prístupových práv a kontroly prístupových účtov a prístupových oprávnení

a

I.1) Sieťová a komunikačná bezpečnosť – Implementácia nástrojov na ochranu integrity sietí, ktoré zabezpečujú riadenie bezpečnostného prístupu medzi vonkajšími a vnútornými sieťami, implementácia segmentácie sietí, implementácia alebo obnova firewall-u, revízia firewall pravidiel.

6. Implementácia systému dvojfaktorovej autentifikácie

Mesto v období 04/2024 realizuje opakovaný audit informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB. Z predbežných zistení vykonaného auditu ako aj z komunikácie s odborne spôsobilými osobami v oblasti vykonávania auditu bolo zistené, že jedným z najväčších nedostatkov úrovne zabezpečenia informačných aktív je nedostatočná vrstva ochrany pri overovaní identity používateľa pri prístupe do siete Mesta. Na základe uvedeného vyššie identifikovaného nedostatku sa Mesto Banská Bystrica snaží reflektovať na „AS-IS" stav a zaviesť dvojfaktorové overovanie, kde okrem súčasného overovania prostredníctvom mena a hesla bude užívateľ nútený zadať generované heslo prostredníctvom SW tokenu a HW tokenu. Mesto Banská Bystrica v rámci zamýšľanej aktivity plánuje obstarať a implementovať systém dvojfaktorovej autentifikácie prostredníctvom obstarania SW / HW tokenov pre celkovo 700 používateľov. Riešenie bude realizované prostredníctvom HW/SW tokenu, ktorý bude generovať jednorazové heslá (OTP – One Time Passwords) pre používateľov prihlasujúcich sa do siete. Používateľ získa OTP prostredníctvom HW zariadenia a SW tokenu nainštalovaného na koncovej stanici. Riadenie identít dvojfaktorového overenia sa plánuje realizovať prostredníctvom platformy nasadenej na infraštruktúre dodávateľa, ktorý zabezpečí s ohľadom na konkrétnu implementáciu nevyhnutné výpočtové zdroje. Súčasťou dodávky bude integrácia dvojfaktorového overovania na jestvujúci systém pre správu identity.

Od implementácie dvojfaktorového overovania Mesto Banská Bystrica očakáva zvýšenie úrovne zabezpečenia prístupu do siete zabezpečením overovania nad rámec súčasného zadávania mena a hesla, keďže v súčasnosti útočníkovi na prístup do siete postačuje získať používateľské meno a heslo bez potreby zadania dynamicky meniaceho sa druhého prihlasovacieho faktoru ako aj zabezpečí súlad so zisteniami opakovaného auditu IB a KB realizovaného v roku 2024.

Aktivita bude pozostávať z obstarania riešenia dvojfaktorovej autentifikácie s celkovým počtom SW/HW tokenov pre 700 používateľov. V rámci aktivity bude vykonaná úvodná analýza, konfigurácia ako aj nasadenie v produkčnom prostredí.

Väzba na oprávnené aktivity z Výzvy: I.2) Sieťová a komunikačná bezpečnosť – Zavedenie bezpečnostných opatrení na bezpečné mobilné pripojenie do siete a vzdialený prístup napríklad implementáciou dvojfaktorovej autentizácie alebo kryptografických prostriedkov.

7. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

Mesto Banská Bystrica momentálne nedisponuje uceleným riešením centrálneho manažmentu a dohľadu nad koncovými stanicami. To má za následok, že ochrana používateľských aktív nie je vzhľadom na rozsah perimetra siete s ohľadom na aktivity vykonávané užívateľmi dostatočná a preto má Mesto ambíciu zvýšiť úroveň zabezpečenia aj na úrovni koncových staníc, čo vníma ako doplňujúcu aktivitu k aktivitám týkajúcich sa výmeny aktívnych sieťových prvkov, riadenia prístupov ako aj segmentácie siete. Mesto vníma potrebu zabezpečiť zlepšenie v oblasti detekcie, investigácie a predikcie pred útokmi na koncové stanice. Z tejto potreby vyplýva potreba nasadenia riešenia, ktoré zabezpečí centrálnu správu ochrany koncových staníc, detekciu nevyžiadanej aktivity, funkcionalitu monitoringu prevádzky na koncovom zariadení a funkcionalitu možnosti centrálneho nastavovania bezpečnostných pravidiel na koncových staniciach. Realizácia tejto aktivity prispeje k holistickému zvýšeniu úrovne zabezpečenia informačných aktív Mesta. Okrem unifikácie a centralizácie zabezpečenia ochrany koncových zariadení aktivita prispeje k zjednodušeniu a systematizácii riadenia ochrany koncových staníc v prostredí Mesta.

Aktivita bude pozostávať z obstarania systému centrálneho dohľadu a manažmentu koncových zariadení pre minimálne 700 koncových staníc. V rámci aktivity bude vykonaná úvodná analýza, konfigurácia ako aj nasadenie v produkčnom prostredí.

Väzba na oprávnené aktivity z Výzvy: H.2) Ochrana proti škodlivému kódu – Implementácia alebo aktualizácia nástrojov na ochranu, ktoré okrem iného vykonávajú kontrolu prístupu k digitálnemu obsahu, pravidelné kontroly úložísk vrátane cloudových riešení, zabraňujú prístupu neoprávnených používateľom filtrovaním obsahu a zamedzením inštalovať alebo odinštalovať alebo zakázať funkcie systému na ochranu škodlivému kódu.

Školenie dotknutého personálu na implementované technológie.

Keďže projekt rieši pomerne širokú škálu činností, ktoré budú mať po úspešnom otestovaní a nasadení dopad na Stakeholderov (prevádzka IKT Mesta a/alebo používateľ koncového zariadenia) bude v rámci dodávok jednotlivých aktivít dodávateľ konkrétneho riešenia súčasne zodpovedný za vykonanie školenia, tak, aby používatelia vedeli výstupy projektu využívať v praxi počas výkonu bežnej agendy. V rámci projektu bude požadované, aby dodávatelia jednotlivých výstupov projektu zabezpečili nevyhnutný rozsah dokumentácie v zmysle Vyhlášky č. 401/2023 Z.z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy v rozsahu minimálnych požiadaviek na dokumentáciu a výstupy relevantné pre školenia.

3.2 Motivácia a rozsah projektu

V rámci Zákona o KB je stanovené, že identifikovaný prevádzkovateľ základnej služby plní požiadavky v nasledujúcom rozsahu:

§ 19 Povinnosti prevádzkovateľa základnej služby

- riešiť kybernetický bezpečnostný incident,
- bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
- spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,
- v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
- oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka, ak sa o ňom hodnoverným spôsobom dozvie

§ 20 Bezpečnostné opatrenia

Najmä pre oblasť:

- § 5 vyhlášky č. 362/2018 Z. z. organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,
- § 6 vyhlášky č. 362/2018 Z. z. riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- § 7 vyhlášky č. 362/2018 Z. z. personálnej bezpečnosti,
- § 8 vyhlášky č. 362/2018 Z. z. riadenia prístupov,§ 9 vyhlášky č. 362/2018 Z. z. riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- § 10 vyhlášky č. 362/2018 Z .z. bezpečnosti pri prevádzke informačných systémov a sietí,
- § 11 vyhlášky č. 362/2018 Z. z. hodnotenia zraniteľností a bezpečnostných aktualizácií,
- § 12 vyhlášky č. 362/2018 Z. z. ochrany proti škodlivému kódu
- § 13 vyhlášky č. 362/2018 Z. z. sieťovej a komunikačnej bezpečnosti,
- § 14 vyhlášky č. 362/2018 Z. z. akvizície, vývoja a údržby informačných sietí a informačných systémov,
- § 15 vyhlášky č. 362/2018 Z. z. zaznamenávania udalostí a monitorovania,
- § 16 vyhlášky č. 362/2018 Z .z. fyzickej bezpečnosti a bezpečnosti prostredia,
- § 17 vyhlášky č. 362/2018 Z. z. riešenia kybernetických bezpečnostných incidentov,
- § 17a vyhlášky č. 362/2018 Z. z. kryptografických opatrení,
- § 17b vyhlášky č. 362/2018 Z. z. riadenia kontinuity prevádzky
- § 17c vyhlášky č. 362/2018 Z. z. auditu, riadenia súladu a kontrolných činností.

Na tieto požiadavky musí Mesto Banská Bystrica neustále reagovať tak, aby bol kontinuálne zabezpečovaný súlad s legislatívnymi požiadavkami. Práve uvedené vyššie je jedným z hlavných motivačných faktorov pre realizáciu uvažovaného projektu.

Motiváciou, prečo realizovať tento projekt je súčasne **celkové zlepšenie úrovne informačnej a kybernetickej bezpečnosti a to prostredníctvom aktivít, ktorých realizácia priamo reflektuje na krátko ako aj strednodobé zistenia a nedostatky v oblasti zabezpečenia informačných aktív Mesta Banská Bystrica ako prevádzkovateľa základnej služby.** Súčasným trendom je zvyšovanie objemu prenášaných údajov internou ale aj verejnou sieťou, nárast veľkosti perimetra siete Mesta, zvyšovanie počtu informačných aktív, či už sa jedná o informačné systémy alebo k nim podporné HW aktíva, čo sa prejavuje v zvyšovaní možností vykonania kybernetického útoku na infraštruktúru Mesta Banská Bystrica. Informačné systémy Mesta podliehajú neustálemu vývoju spojenému so zmenou, pričom frekvencia zmien má rovnako vzrastajúci trend, na čo Mesto Banská Bystrica musí pružne reagovať. Okrem vyššie uvedeného, aktíva Mesta interagujú s ďalšími systémami, ktoré sú z pohľadu Mesta v postavení externých systémov a služieb, či už na strane štátu alebo tretích strán z komerčného sektora. Aj nárast počtu integrácií a rozhraní s ktorými aktíva Mesta priamo alebo nepriamo interagujú vyvoláva zvýšenú potrebu nie len na bezpečnosť samotnú, ale aj dostupnosť a kvalitu poskytovaných ako aj konzumovaných služieb. Tento holistický pohľad na potrebu zabezpečenia vysokej úrovne kybernetickej i informačnej bezpečnosti aktív Mesta Banská Bystrica dáva za pre misiu Mesta poskytovať služby nie len bezpečné, ale aj kvalitné a dostupné.

Realizáciou navrhovaných aktivít projektu sa dosiahne vyriešenie nasledovných problémov:

1. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB

- Splnenie legislatívnej požiadavky na pravidelný výkon auditu informačnej a kybernetickej bezpečnosti;
- Odpočet pôvodných zistení ako aj identifikácia nových zistení, na ktoré je potrebné reflektovať;
- Zvýšenie efektu realizácie navrhovaných aktivít v tomto Projektovom zámere prostredníctvom zohľadnenia výstupov auditu – podpora prioritizácie oblastí zamerania sa projektu s ohľadom na dostupné technické / personálne / finančné kapacity Mesta.
- Získanie uceleného aktuálneho prehľadu o stave zabezpečenia IB a KB.

2. Vypracovanie relevantnej bezpečnostnej dokumentácie

- Zlepšenie transparentnosti a bezpečnostných postupov Mesta ako organizácie v oblasti postupov, politík a procesov v oblasti IB a KB;
- Zníženie rizík a ochrana pred hrozbami vplyvom minimalizácie rizika úniku citlivých údajov, ktoré sú zberané, vytvárané, spracúvané, uchovávané, zdieľané v rámci informačných aktív Mesta;
- Zlepšenie konzistencie a súlad s legislatívou, zabezpečenie konzistentnosti v návrhu, organizácii a implementácii procesov a bezpečnostných politík a tým zameranie sa na dodržiavanie predpisov a štandardov v oblasti IB a KB.
- Zlepšenie procesu riadenia rizík vďaka identifikovaným a vyhodnoteným rizikám, ktorým Mesto Banská Bystrica čelí.

- Jasne a jednoznačne zadefinované interné postupy, smernice a stratégie, ktoré zohľadňujú aktuálny stav zabezpečenia informačných aktív Mesta ako aj súčasné legislatívne požiadavky kladené na Mesto ako prevádzkovateľa základnej služby;
- Zníženie pravdepodobnosti vzniku bezpečnostných incidentov vďaka implementácii definovaných postupov a opatrení uvedených vo vypracovanej bezpečnostnej dokumentácii;
- Zvýšenie celkovej úrovne zabezpečenia Mesta Banská Bystrica prostredníctvom vykonanej identifikácie a analýzy potenciálnych bezpečnostných hrozieb a zraniteľností v informačných systémoch Mesta. Prostredníctvom implementácie odporúčaných opatrení a postupov sa bude Mesto Banská Bystrica ako prevádzkovateľ základnej služby efektívnejšie brániť proti identifikovaným bezpečnostným hrozbám;
- Realizáciou tejto aktivity sa okrem naplnenia minimálnych požiadaviek poskytovateľa NFP odstráni aktuálny stav v oblasti governance informačnej a kybernetickej bezpečnosti, kedy Mesto okrem zriadeného Bezpečnostného výboru nedisponuje žiadnou vypracovanou bezpečnostnou dokumentáciou a teda riadenie IB a KB sa zmení z neformálne riadeného na formálne a procesne riadené s jasne popísanými úrovňami zodpovedností a právomocí;

3. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta

- Nasadením platformy pre správu prístupov sa napomôže vyriešiť problém neoprávneného prístupu k sieti pomocou autentifikácie a autorizácie používateľov a zariadení a odstráni sa súčasný stav, ktorý sa vyznačuje nízkou efektivitou a nízkou flexibilitou pri správe identít a prístupových práv v sieti;
- Rozšíria sa možnosti kategorizácie používateľov a zariadení (profilácia), čím Mesto Banská Bystrica nadobudne väčšiu flexibilitu selekcie prideľovania prístupov vybraným typom používateľov a/alebo zariadení;
- Zvýšenie úrovne zabezpečenia pred bezpečnostnými hrozbami prostredníctvom zvýšenia počtu a dostupnosti prístupových politík a politík kontroly, čím sa zníži riziko neoprávneného prístupu do siete Mesta;
- Odstránenie súčasne nízkeho stavu auditovateľnosti prihlasovania sa používateľov a/alebo zariadení do siete Mesta;
- Zjednodušenie riadenie prístupu pre rôzne typy používateľov a zariadení za súčasného odbúravania agendy personálu zodpovedajúceho za prevádzku IKT, IB a KB;
- Výmenou switchov, ktoré sú end-of-sale a end-of-support za nové, ktoré majú podporu protokolu IEEE 802.1X sa zníži riziko výpadkov v sieti, zabezpečí kontinuita podpory a záplat na HW infraštruktúre ako aj súlad so všeobecne platnými praktickými pravidlami potreby nahradiť end-of-support produkty za tie, ktoré sú podporované.

4. Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky

- Vykonaním segmentácie siete Mesta Banská Bystrica sa odstráni súčasný stav, kedy sa v prípade úspešného útoku tento má možnosť šíriť po celej sieti. Realizáciou segmentácie sa dosiahne stav, kedy sa zúži možnosť šírenia útokov a hrozieb na úroveň vytvorených segmentov;
- Segmentácia prispeje k odstráneniu stavu, kedy autorizovaný a autentifikovaný užívateľ má prístup do celej siete a nie iba do časti, do ktorej má mať prístup vzhľadom na jeho príslušnosť do skupiny používateľov / zariadení;
- Vykonaním segmentácie siete sa očakáva optimalizácia výkonu siete a to oddelením prevádzky prioritných aktív od menej prioritných;
- Zjednodušenie a zrýchlenie diagnostiky siete po vykonaní segmentácie vzhľadom na skutočnosť, že po vykonaní segmentácie bude možné jednoduchšie lokalizovať a diagnostikovať prípadné problémy so sieťovou dostupnosťou alebo výkonom na úrovni konkrétneho segmentu siete;

5. Dodávka aktívnych prvkov CORE časti siete

- Nákupom nových aktívnych prvkov CORE časti siete Mesta sa zníži riziko výpadkov v sieti, zabezpečí kontinuita podpory a záplat na CORE HW sieťovej infraštruktúre, nakoľko v súčasnosti Mesto Banská Bystrica na úrovni CORE časti siete disponuje zariadeniami, ktoré sú end-of-sale a end-of-support;
- Nákupom nových aktívnych prvkov sa doplní CORE časť siete, čím sa podporí zabezpečenie kontinuity požadovanej úrovne IT aktív, ako aj primerané doby odozvy informačných aktív v sieti Mesta;
- Jedným z hlavných problémov, ktorý rieši táto aktivita je, že nové zariadenia pre CORE časť siete umožnia vykonať realizáciu aktivity č.3 ako aj č.4 keďže nové zariadenia budú podporovať protokol IEEE 802.1X pre účely nasadenia systému riadenia a správy prístupov koncových zariadení a to aj v kontexte uvažovanej segmentácie siete;
- Nákupom nových aktívnych prvkov CORE časti siete sa súčasne očakáva zvýšenie úrovne spoľahlivosti siete, keďže Mesto Banská Bystrica očakáva, že nové, výrobcom podporované a moderné aktívne prvky disponujú vyššou mierou odolnosti voči výpadkom a poruchám v porovnaní s jestvujúcimi zariadeniami.

6. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

- Implementáciou systému dvojfaktorového overovania Mesto Banská Bystrica očakáva zvýšenie úrovne zabezpečenia prístupu používateľov do siete prostredníctvom pridania ďalšieho faktora overenia voči súčasnému stavu, ktorý od užívateľov vyžaduje pri prihlásení sa do siete iba kombináciu mena a hesla, čo môže napr. pri phisingovej kampani útočník prelomiť a získať prístup k aktívam Mesta bez potreby vykonania ďalšieho kroku pri prístupe do siete;
- Implementáciou riešenia sa očakáva súčasne dodržiavanie bezpečnostných predpisov a noriem resp. zistení, ktoré boli identifikované počas vykonávaných auditov KB. Zodpovedný certifikovaný audítor opakovane v zisteniach uviedol nevyhnutnosť zabezpečenia prístupu do siete Mesta prostredníctvom zavedenia ďalšieho faktora overovania. Na základe uvedeného Mesto túto aktivitu považuje za absolútne kľúčovú, keďže dlhodobým zámerom mesta je držať vysokú úroveň IB a KB aj v kontexte identifikovaných zistení.
- Zavedením dvojfaktorového overovania sa zároveň zvýši úroveň zabezpečenia vzdialeného prístupu do siete Mesta z externého prostredia, ktorého úroveň zabezpečenia nemá Mesto pod kontrolou.

7. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

- Nasadením riešenia centrálneho bezpečnostného manažmentu pre koncové stanice Mesto Banská Bystrica zvýši úroveň zabezpečenia koncových staníc ako aj zvýši efektivitu riadenia prevádzky koncových staníc, nakoľko realizáciou tejto aktivity očakáva nadobudnutie možnosti centralizovanej správy zariadení ako aj centrálneho sledovania správania na koncových staniciach;

- Riešenie zvýši viditeľnosť personálu zodpovedného za riadenie prevádzky a správy aktív ako aj IB a KB, nakoľko riešenie prinesie zvýšenú úroveň a granularitu monitoringu koncových staníc ako aj získanie informácií o klientoch na koncových staniciach v reálnom čase;
- Súčasne bude prevádzkový personál disponovať nástrojom, ktorý generuje notifikácie v prípade výskytu neočakávaných situácií, čo rovnako zvýši možnosť koncentrovať sa udalosti s vyššou prioritou;

Podpora business procesov

Realizáciou aktivít projektu nedôjde k zmenám na strane súčasne nastavených business procesov. Jednotlivé organizačné útvary mesta, ako aj organizácie v zriaďovateľskej pôsobnosti mesta, príspevkové organizácie, ktoré realizujú business procesy na dennej báze nebudú v oblasti výkonu ich nastavených business procesov priamo ovplyvnené. Realizácia aktivít projektu bude mať predovšetkým podporný charakter, keďže plošne na úrovni siete Mesta Banská Bystrica budú zabezpečené informačné aktíva, ktoré sú využívané v jednotlivých vykonávaných business procesoch vykonávaných v rámci ISVS, ktoré Mesto Banská Bystrica súčasne uvádza v META IS:

Názov	Kód Meta IS	Stav
Mobilná aplikácia RON	Isvs_11928	V prevádzke
RON Jedáleň aplikácia	Isvs_11927	V prevádzke
RON jedálenský systém	Isvs_11926	V prevádzke
RON dochádzkový systém	Isvs_11925	V prevádzke
Pohoda – ekonomický softvér	Isvs_11924	V prevádzke
SPIN – pult centrálnej ochrany MsP	Isvs_11917	V prevádzke
SHERIFF – IS mestskej polície	Isvs_11916	V prevádzke
MS Office365	Isvs_11915	V prevádzke
IS HER pre rokovanie MsR a MsZ	Isvs_11914	V prevádzke
GScan – scanovací modul	Isvs_11913	V prevádzke
GISPlan – geograficky IS	Isvs_11912	V prevádzke
eZákazky – softvér	Isvs_11911	V prevádzke
Systém pre verejné obstarávanie – eBiz	Isvs_11910	V prevádzke
aScOrbit	Isvs_11909	V prevádzke
aSc Agenda	Isvs_11908	V prevádzke
Webové sídlo Mesta Banská Bystrica	Isvs_11907	V prevádzke
Registratúrny systém CG DISS	Isvs_11906	V prevádzke
Intranetový Portál mesta	Isvs_11904	V prevádzke
Portálový modul CG Datamesta	Isvs_11903	V prevádzke
Portálový modul CG eGOV	Isvs_11902	V prevádzke
Modul integrácie na externé IS .COMM ISS	Isvs_11901	V prevádzke
Personalistika a mzdy CG ISS	Isvs_11900	V prevádzke
Ekonomika CG ISS	Isvs_11899	V prevádzke
BASE CG ISS	Isvs_11898	V prevádzke
Informačný systém mesta CG ISS	Isvs_11897	V prevádzke
Informačný systém Digitálna technická mapa a digitálny územný plán	Isvs_11468	V pláne vybudovať
Podpora asistovaného života seniorov	Isvs_11066	V pláne vybudovať
Manažment s podporou IoT	Isvs_11065	V pláne vybudovať
Platforma SMART CITY	Isvs_10386	V prevádzke

Na základe uvedeného možno sumarizovať nasledovné hlavné business procesy, ktoré budú podporené zvýšenou úrovňou zabezpečenia:

- Správa financií a rozpočtu;
- Správa miestnych poplatkov a daní (registrovanie a výber poplatkov za psa);
- Riadenie a kontrola dochádzky zamestnancov;
- Výkon dohľadu nad bezpečnosťou verejných priestranstiev;
- Riadenie procesu obstarávania tovarov, služieb a stavebných zákaziek;
- Personálna a mzdová agenda;
- Správa mestskej infraštruktúry a stavebná agenda (zriaďovanie vecného bremena na majetok Mesta / vydávanie rozhodnutí o zvláštnom užívaní miestnej komunikácie /);
- Matrika – evidencia udalostí, správa evidencie a údajov o identite a občianstve, vybavovanie žiadostí;
- Sociálna agenda a školstvo;
- Agenda životného prostredia (vydávanie rozhodnutí o výrube dreviny)
- Agenda dopravy (vyhradzovanie parkovacieho miesta za poplatok / vydávanie parkovacej karty / určovanie trvalého alebo prenosného dopravného značenia);

Podrobný zoznam business procesov realizovaných prostredníctvom identifikovaných ISVS je možné stotožniť s poskytovanými koncovými službami Mesta, ktorých podrobný zoznam je uvedený tu: https://metais.vicepremier.gov.sk/detail/PO/63fd37ae-5ee8-413d-9141-c259f190d310/cimaster?tab=relationsForm.

Realizácia projektu ako aj jeho očakávané výsledky a výstupy priamo nerieši životné situácie, ich organizáciu a charakter a ani nevytvára zmeny v jestvujúcich životných situáciách prostredníctvom ktorých interaguje Mesto Banská Bystrica s obyvateľmi, návštevníkmi alebo podnikateľskou sférou. Zvýšenie úrovne kybernetickej a informačnej bezpečnosti nevyvolá zmenu charakteru poskytovaných služieb horeuvedeným skupinám, ale prispeje k zvýšeniu úrovne zabezpečenia informačných aktív, ktoré sú pri výkone agendy v oblasti životných situácií využívané. Možno konštatovať, že projekt zabezpečí okrem vyššej úrovne bezpečnosti aj vyššiu úroveň odolnosti služieb a teda aj ich celkovej dostupnosti pre dotknutých stakeholderov. Horeuvedené ISVS tak zvýšia stabilitu poskytovaných služieb mesta napr. pri nasledovných životných situáciách:

- Narodenie dieťaťa;
- Úmrtie;
- Zmena osobných údajov;
- Zmena trvalého / prechodného pobytu...

Motiváciou na dosiahnutie budúceho požadovaného stavu bolo predovšetkým nasledovné:

- Ambícia Mesta Banská Bystrica reflektovať na aktuálne hrozby a výzvy v oblasti IB a KB;
- Zrealizovaný a vykonávaný audit KB;
- Ochrana reputácie Mesta Banská Bystrica ako prevádzkovateľa základnej služby;
- Ochrana dôvernosti a integrity údajov spracúvaných v informačných aktívach Mesta;
- Dodržiavanie súladu s aktuálne platnou legislatívou;
- Zabezpečenie kontinuity prevádzky informačných aktív;
- Zlepšenie internej efektivity a efektívnosti pri správe a dohľade nad informačnými aktívami Mesta.

3.3 Zainteresované strany/Stakeholderi

ID	AKTÉR / STAKEHOLDER	SUBJEKT (názov / skratka)	ROLA (vlastník procesu/ vlastník dát/zákazník/ užívateľ .... člen tímu atď.)	Informačný systém (MetaIS kód a názov ISVS)
1.	Mesto Banská Bystrica	Mesto BB	Vlastník informačných aktív a monitorovaný subjekt, prevádzkovateľ základnej služby	Viď tabuľka - časť 3.2 tohto dokumentu
2.	Ministerstvo investícií, regionálneho rozvoja a informatizácie SR	MIRRI	Gestor eGovernmentu, riadiaci orgán	Nerelevantné
3.	Občan/podnikateľ/návštevník mesta	FO/PO	užívateľ	Nerelevantné
4.	Orgány verejnej moci a ich podsektory	OVM	Zdieľanie dát medzi ISVS OVM a ISVS Mesta BB	

3.4 Ciele projektu

ID	Názov cieľa	Názov strategického cieľa	Spôsob realizácie strategického cieľa
1.	Zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.	Zabezpečiť primeranými technickými, organizačnými a personálnymi bezpečnostnými opatreniami ochranu dôvernosť, integrity a dostupnosti informačných aktív (Stratégia KB, MIRRI)	1. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 9 Zákona o KB; 2. Vypracovanie relevantnej bezpečnostnej dokumentácie; 3. Implementácia systému pre inventarizáciu aktív a harmonizáciu procesov v oblasti IB a KB; 4. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica; 5. Vykonanie segmentácie siete Mesta Banská Bystrica s ohľadom na súčasné prevádzkové požiadavky; 6. Výmena aktívnych prvkov CORE časti siete;

			7. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete; 8. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice;
2.	Zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.	Zvyšovať povedomie o informačnej a kybernetickej bezpečnosti všetkých zamestnancov a vedenia organizácie	Realizácia školenia dotknutého personálu na implementované technológie.

3.5 Merateľné ukazovatele (KPI)

ID	ID/Názov cieľa	Názov ukazovateľa (KPI)	Popis ukazovateľa	Merná jednotka	AS IS merateľné hodnoty (aktuálne)	TO BE Merateľné hodnoty (cieľové hodnoty)	Spôsob ich merania	Pozn.
1.	PO095/PSKP S0I12	Verejné inštitúcie podporované v rozvoji kybernetických služieb, produktov a procesov	Počet verejných inštitúcií, ktoré sú podporované za účelom rozvoja a modernizácie kybernetických služieb, produktov, procesov a zvyšovania vedomostnej úrovne, napríklad v kontexte opatrení smerujúcich k elektronickej verejnej správy.	Verejné inštitúcie	0	1	Preverí sa, skutočný počet podporených subjektov verejnej správy zapísaných v štatistickom registri organizácií vedenom Štatistickým úradom SR, ktoré sú zaradené v sektore verejnej správy, v rámci ktorých došlo k modernizácii služieb, produktov, procesov a zvýšeniu vedomostnej úrovne v kontexte opatrení smerujúcich k elektronickej bezpečnosti verejnej správy	Aktivity projektu realizované na úrovni Mesta Banská Bystrica.
2.	PR017/PSKP RCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Počet nových a vylepšených verejných digitálnych služieb, produktov a procesov	Používatelia / rok	0	250	Preverí sa, počet zamestnancov, ktorí sú používateľmi nových a vylepšených digitálnych služieb	„TO-BE" bude zodpovedať počtu zamestnancov, ktorí vykonávajú svoje činnosti na zabezpečených informačných aktívach, ktorých zabezpečenie je predmetom projektu.
3.	PR017 / PSKPRCR11	Používatelia nových a vylepšených verejných digitálnych služieb, produktov a procesov	Nová verejná digitálna služba, produkt alebo proces	Používatelia / rok	0	250	Preverí sa počet zamestnancov, ktorí sú používateľmi novej verejnej digitálnej služby, produktu alebo procesu	Nové produkty ako výsledok projektu, preverí sa preukázaním dokumentácie a/alebo prostredníctvom preberacích protokolov a/alebo dátových

								listov k dodaným produktom.

3.6 Špecifikácia potrieb koncového používateľa

n/a

3.7 Riziká a závislosti

Vo procese spracovania tohto dokumentu Mesto Banská Bystrica identifikovalo nasledovné riziká:

A. Omeškanie alebo zrušenie procesu verejného obstarávania;
B. Personálne kapacity na strane Mesta Banská Bystrica;
C. Kapacity a odbornosť na strane dodávateľa/dodávateľov;
D. Havária niektorého z dotknutých ISVS alebo časti siete nezapríčinená Mestom a/alebo dodávateľom/dodávateľmi;
E. Legislatívne zmeny, zmeny v riadiacej dokumentácii.

Podrobnejšie informácie o rizikách a závislostiach sú uvedené v samostatnom dokumente „Zoznam rizík a závislosti", ktorý bude počas ďalších etáp projektu aktualizovaný na pravidelnej báze. Súčasne budú riziká vyhodnocované na dvoch úrovniach:

- „high-level" – riziká s dopadom na realizáciu plánu projektu a progresu projektových aktivít;
- „low-level" – riziká s menším dopadom a dopadom predovšetkým na úrovni dodávky predmetu projektu „delivery level".

Procesné riadenie rizík bude podrobne popísané v rámci Projektového iniciálneho dokumentu („PID"), v prípade, že bude projekt oficiálne spustený. V rámci PID budú definované spôsoby a stratégie riadenia rizík ako aj ich komunikácie v priebehu celého projektu.

3.8 Stanovenie alternatív v biznisovej vrstve architektúry

Na riešenie problémovej situácie boli identifikované možné alternatívne/variantné riešenia:

	Budúci možný stav			
Súčasný stav	**Možný variant**	**Biznis vrstva**	**Aplikačná vrstva**	**Technologická vrstva**
Nedostatočná úroveň zabezpečenia IB a KB v Meste Banská Bystrica	Nulový variant	Pokračovať v súčasnom stave bez nutnosti realizácie projektu	Využiť súčasnú, pre realizáciu všetkých aktivít projektu nepostačujúcu, úroveň aplikačnej vrstvy pri zachovaní stavu „AS-IS"	Realizovať len nákup HW s obmedzenom počte sieťových prvkov bez výmeny aktívnych prvkov bez podpory IEEE 802.1X
	Optimálny variant (celý rozsah projektu)	**Realizovať projekt v plnom rozsahu**	**Doplniť súčasnú aplikačnú vrstvu o nové prvky potrebné pre zvýšenie úrovne IB a KB a vykonať implementáciu a konfiguráciu služieb tak, aby bol využitý maximálny potenciál a funkcionalita súčasných ako aj navrhovaných riešení**	**Implementovať všetky funkcionality, kompletný rozsah nástrojov a vytvoriť bezpečný kybernetický priestor**
	Limitovaný variant	Pre realizáciu projektu využiť len realizáciu vybraných aktivít dvojfaktorové overovanie, realizácia opakovaného auditu KB a vypracovanie relevantnej bezpečnostnej dokumentácie	Nasadiť iba moduly s obmedzenou funkcionalitou, resp. vybrať iba tie, ktoré sú z pohľadu vykonaného auditu KB s najvyššou prioritou (riešenie 2 faktorovej autentifikácie)	Realizovať len nákup HW komponentov potrebných pre implementáciu dvojfaktorového overovania, bez výmeny HW v CORE časti siete a výmeny zariadení s podporou IEEE 802.1X

Pri realizácii projektu je možné na základe vykonanej analýzy postupovať troma nasledovnými alternatívami:

A. **Nulový variant:** Zachovať súčasný stav, a jednotlivé navrhované aktivity projektu realizovať čiastkovo bez vzájomného koordinovaného postupu. Tento variant je síce najlacnejší z pohľadu úspor za nezrealizované aktivity, avšak navrhované aktivity projektu reflektujú legislatívne požiadavky a povinnosti Mesta Banská Bystrica na zabezpečenie svojich informačných aktív. Je dôvodné očakávať, že nerealizovanie projektu (akceptácia nulového variantu) by viedla k dodatočným nákladom presahujúcim nakumulované úspory – neodporúča sa.

B. **Optimálny variant:** Realizácia aktivít projektu v celom ich rozsahu so zohľadnením východiskového stavu. Aktivity projektu boli volené na základe skutočných potrieb Mesta Banská Bystrica a dôrazom na ich vzájomné prepojenie, preto je účelné ich realizovať v rámci jedného projektu vo vzájomne súvisiacich pracovných balíkoch. Realizácia projektu v optimálnom variante zároveň vyrieši všetky súčasne identifikované zásadné nedostatky v oblasti IB a KB, ktoré sú Mestu známe.

C. **Obmedzený variant:** Tento variant počíta s realizáciou aktivít projektu s najvyššou prioritou a to i napriek tomu, že všetky navrhované aktivity možno považovať za prioritné. V tomto variante sa počíta s nasadením riešenia dvojfaktorovej autentifikácie ako niekoľkokrát opakovaného zistenia auditov KB, súčasne navrhuje realizáciu resp. ukončenie opakovaného auditu, ktorý bol zahájený po 20.02.2024 ako aj s vypracovaním relevantnej bezpečnostnej dokumentácie na úrovni organizácie, keďže Mesto ňou v súčasnosti nedisponuje. V tomto variante sa

D. nepočíta s nákupom HW komponentov s podporou IEEE 802.1X a súvisiacimi aktivitami ako segmentácia siete. V tomto prípade, by síce došlo k odstráneniu zásadných nedostatkov identifikovaných auditmi KB, avšak úroveň IB a KB by nebola zabezpečená na takej úrovni ako je účelné ju riešiť v optimálnom variante a to aj z dôvodu, že jednotlivé aktivity sú navzájom v prieniku, čo pri súčasnej implementácii povedie k úspore min. v oblasti riadenia projektu. Zároveň je možné očakávať, že nerealizované aktivity v tomto variante bude potrebné tak či onak realizovať, pričom nemožno očakávať, že ich realizácia v budúcnosti bude možná za rovnakých alebo výhodnejších podmienok.

Odporúčanie: Navrhuje sa realizovať Optimálny variant.

3.9 Multikriteriálna analýza

Kritériá pre MCA

	KRITÉRIUM	ZDÔVODNENIE KRITÉRIA	Občan / podnikateľ	Zamestnanec	Mesto BB	Podriadené organizácie
Stanovené alternatívy	Kritérium A (KO) - komplexná identifikácia aktuálnych hrozieb	Realizácia projektu zabezpečí komplexnú analýzu a následnú identifikáciu hrozieb, ktoré prispeje k efektívnemu nasadzovaniu preventívnych opatrení		X	X	X
	Kritérium B (KO) - súlad s legislatívnymi požiadavkami na úrovni governance a procesov v oblasti IB a KB	Zabezpečí sa vypracovanie kompletnej dokumentácie v súlade s aktuálne platnou legislatívou v oblasti IB a KB ako aj vypracovanie interných riadiacich aktov pre oblasť IB a KB		X	X	X
	Kritérium C (KO) - zabezpečenie vyššej úrovne prístupu do siete	Prispeje k posilneniu bezpečnosti pri prístupe používateľov do siete o pridanie druhého faktora		X	X	X
	Kritérium D -lepšie a efektívnejšie využite nových technológií	Nové funkcionality výrazne zvyšujú schopnosť ochrany pred kybernetickými bezpečnostnými incidentami		X	X	X
	Kritérium E Vytvorenie pokročilého systému autentifikácie a autorizácie v sieti mesta na úrovni skupín používateľov	Riadenie prístupov do siete Mesta Banská Bystrica vrátane vykonania segmentácie, tvorby skupín zariadení a používateľov (profily), zabezpečenie prístupov zariadení a používateľov na úrovni portu na aktívnom prvku	X	X	X	X

	Kritérium F Centralizovaný dohľad a správa nad informačnými aktívami	Zabezpečenie nástrojov na ochranu, monitoring a centrálny dohľad nad aktívami Mesta Banská Bystrica		X	X	X

Vyhodnotenie MCA

Zoznam kritérií	Alternatíva1	Spôsob dosiahnutia	Alternatíva 2	Spôsob dosiahnutia	Alternatíva 3	Spôsob dosiahnutia
Kritérium A	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 zabezpečí komplexnú analýzu a identifikáciu hrozieb	áno	Implementácia alternatívy č. 3 zabezpečí komplexnú analýzu a identifikáciu hrozieb
Kritérium B	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 zabezpečí vypracovanie kompletnej dokumentácie v súlade s aktuálne platnou legislatívou v oblasti IB a KB ako aj vypracovanie interných riadiacich aktov pre oblasť IB a KB	áno	Implementácia alternatívy č. 3 zabezpečí vypracovanie kompletnej dokumentácie v súlade s aktuálne platnou legislatívou v oblasti IB a KB ako aj vypracovanie interných riadiacich aktov pre oblasť IB a KB
Kritérium C	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 Prispeje k posilneniu bezpečnosti pri prístupe používateľov do siete o pridanie druhého faktora overenia	áno	Implementácia alternatívy č. 3 Prispeje k posilneniu bezpečnosti pri prístupe používateľov do siete o pridanie druhého faktora overenia
Kritérium D	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 pomocou implementácie nových funkcionalít navrhovaných projektom výrazne zvýši schopnosť ochrany pred kybernetickými bezpečnostnými incidentami	Čiastočne áno	Implementácia alternatívy č. 3 pomocou nových funkcionalít v obmedzenom rozsahu zvýši čiastočne schopnosť ochrany pred kybernetickými bezpečnostnými incidentmi.
Kritérium E	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 Zabezpečí riadenie prístupov do siete Mesta Banská Bystrica vrátane vykonania segmentácie, tvorby skupín zariadení a používateľov (profily), zabezpečí prístupy zariadení a používateľov na úrovni portu na aktívnom prvku	nie	Zachovanie súčasného stavu
Kritérium F	nie	Zachovanie súčasného stavu	áno	Implementácia alternatívy č. 2 Zabezpečí nástroje na ochranu, monitoring a centrálny dohľad nad aktívami Mesta Banská Bystrica	nie	Zachovanie súčasného stavu

3.10 Stanovenie alternatív v aplikačnej vrstve architektúry

Alternatívy na úrovni aplikačnej architektúry reflektujú alternatívy vypracované na základe „nadradenej" architektonickej biznis vrstvy, pričom vďaka uplatneniu nasledujúcich princípov aplikačná vrstva architektúry dopĺňa informácie k alternatívam stanoveným pomocou biznis architektúry.

V nadväznosti na stanovenie alternatív business vrstvy, za najvýhodnejšiu sa v kontexte legislatívnych požiadaviek, východiskového stavu, prevádzkových a administratívnych nákladov považuje Alternatíva č.2.

3.11 Stanovenie alternatív v technologickej vrstve architektúry

Výber alternatívy na úrovni technologickej vrstvy reflektuje a kopíruje výber Alternatívy č.2 na základe MCA. Riešenie Alternatívy č.2 (ako aj ostatné uvažované alternatívy) sa plánuje nasadiť na infraštruktúre Mesta Banská Bystrica. Všetky HW komponenty, ktoré sú predmetom projektu budú fyzicky dodané, umiestnené a inštalované v prostredí Mesta.

S využitím vládneho cloudu sa aj s ohľadom na charakter projektu nepočíta. Z ohľadom na uvedené nebolo nutné vykonať analýzu posúdenia finančnej udržateľnosti a výhodnosti riešenia vládneho cloudu vo vzťahu k iným alternatívam.

Celkové výdavky projektu v štandardizovanom členení, t.j. s uvedením CAPEX a OPEX sú uvedené nižšie v tomto dokumente v časti „Rozpočet projektu".

4. POŽADOVANÉ VÝSTUPY (PRODUKT PROJEKTU)

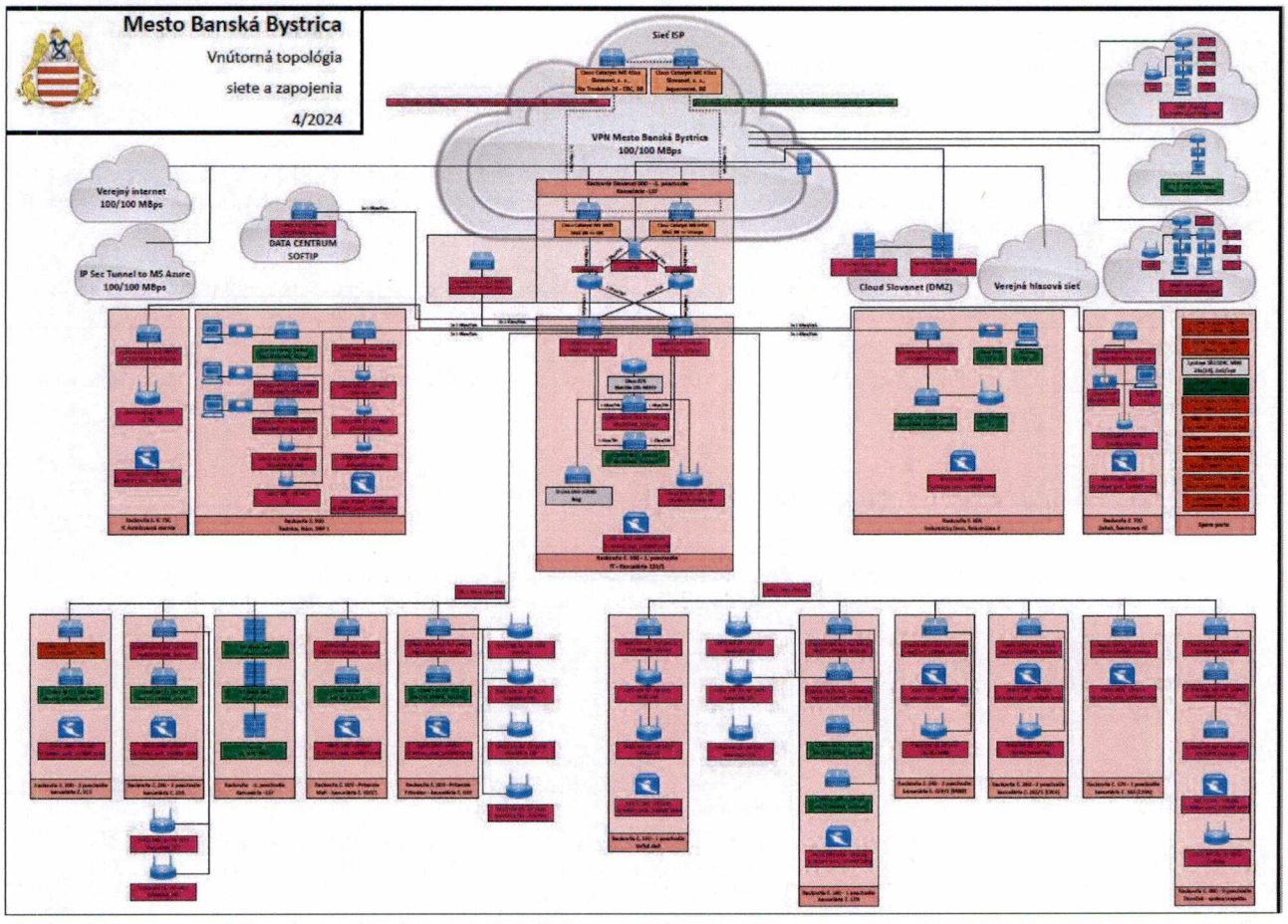
Požadovaným výstupom projektu je funkčné, dlhodobo udržateľné a ucelené riešenie pre zvýšenie úrovne IB a KB, ktoré pozostáva z viacero navzájom súvisiacich produktov projektu. Podrobnejší popis výstupov projektu sumarizuje nasledovná tabuľka:

ID	Výstup projektu – názov	Popis / poznámka
1.	Vykonaný opakovaný audit projektu	Výstupom opakovaného auditu bude správa audítora KB v súlade so Zákonom o KB
2.	Vypracovaná bezpečnostná dokumentácia	Výstupom bude vypracovaná bezpečnostná dokumentácia v súlade so Zákonom o KB a Vyhláškou o KB v rozsahu uvedenom v časti 3 tohto dokumentu
3.	Nasadené riešenie správy prístupov koncových zariadení do siete Mesta	Výstupom bude nasadené riešenie správy prístupov koncových zariadení do siete Mesta založené na protokole IEEE 802.1X vrátane dodávky 7 ks switchov, ktoré podporujú protokol 802.1X.
4.	Vykonaná segmentácia siete	Výstupom projektu bude vykonaná segmentácia siete v súlade s vykonanou analýzou, ktorú zabezpečia externé kapacity dodávateľa na základe získaných informácií počas etapy analýza a dizajn. Výstupom bude súčasne konfiguračná dokumentácia.
5.	Dodané aktívne prvky CORE časti siete	Výstupom bude dodaných celkovo 9 ks aktívnych sieťových prvkov s podporou IEEE 802.1X.
6.	Nasadený systém dvojfaktorovej autentifikácie	Výstupom bude nasadený systém dvojfaktorovej autentifikácie s klientami a tokenmi pre 700 používateľov (50 ks HW token + 650 ks SW token).
7.	Nasadené riešenie centrálneho bezpečnostného manažmentu	Výstupom bude nasadený systém uceleného riešenia centrálnej správy koncových staníc pre 700 ks koncových staníc.
8.	Projektové výstupy – dokumentácia	Výstupom bude súbor dokumentácie vypracovanej v zmysle Vyhlášky 401/2023 Z.z. o riadení projektov v rozsahu a kontexte zodpovedajúcemu rozsahu projektu. Ucelený zoznam požadovaných výstupov (produktov projektu vrátane manažérskych produktov) bude uvedený v Projektovom iniciálnom dokumente („PID") v následnej fáze projektu.

Výstupmi projektu nebudú žiadne koncové služby ani biznis objekty, ktoré možno klasifikovať ako výstupy zo systému (napr. podania, formuláre, rozhodnutia, reporty, dáta, aplikačné rozhrania...). Vlastníkom výstupov ako aj procesu bude zástupca Mesta, ktorý bude súčasne zastávať pozíciu kľúčového používateľa.

5. NÁHĽAD ARCHITEKTÚRY

V náhľade nižšie uvádzame pohľad na komplexnú sieťovú architektúru Mesta. Realizáciou aktivít projektu nedôjde k zmene topológie siete, ani zmene na úrovni dátovej architektúry.



Zmeny na úrovni business architektúry budú minimálne a to vo väzbe na nutnosť zadávania druhého faktora v riešení dvojfaktorového overovania, kedy používateľ okrem mena a hesla bude nútený zadať druhý prístupový kód generovaný HW alebo SW tokenom.

Platforma pre správu prístupov:

Centralizovaný manažment a správa	• centrálna konfigurácia a správa profilov, prístupov, hostí, autentifikácia a autorizácia služieb v jednoduchom web grafickom rozhraní;
Riadenie politík	• možnosť nastavovania politík prístupu na základe definovaných pravidiel; • možnosť tvorby modelov prístupu na základe definície rôznych atribútov ako sú identita používateľa / zariadenia, autentifikačné protokoly, identita koncového zariadenia; • možnosť dynamickej definície a nastavovania atribútov; • možnosť integrácie na Microsoft Active Directory, LDAP, RADIUS, RSA OTP.
Riadenie prístupov	• na základe Access Control Lists (dACLs), priradeniu k VLAN, URL presmerovania, ACLs, SGACLs.
Riadenie šifrovania	• možnosť editácie zoznamu používaného šifrovania, ktoré môže byť zakázané pre účely vynútenia bezpečnostných politík organizácie; • možnosť vynútenia využívania povoleného typu šifrovania pri autentifikácii.
AI/ML profilovanie a viacfaktorová klasifikácia	• možnosť rýchlej identifikácie neznámych koncových zariadení prostredníctvom cloudového ML engine; • možnosť revízie zariadení prostredníctvom profilových politík použitím ML engine; • možnosť tvorby prístupových skupín koncových zariadení prostredníctvom profilov a pravidiel vytvorených správcom siete;
Prístup do siete	• možnosť rýchleho nasadenia zabezpečeného prístupu k sieti prostredníctvom autentifikácie a autorizácie na základe údajov získaných z prihlasovacích údajov na rôznych aplikačných úrovniach.
Riadenie politiky prístupových skupín	• podpora jednoduchej segmentácie prostredníctvom bezpečnostných tagov; • funkcionalita správy segmentácie a zjednodušenej správy prepínačov, smerovačov, bezdrôtových zariadení a pravidiel pre firewally.

Pridávanie zariadení do siete	• podpora automatizovaného poskytovania a registrácie certifikátu pre štandardné PC a mobilné zariadenia;
AAA služby	• podpora RADIUS protokolu pre autentifikáciu, autorizáciu a accouting (AAA); • podpora protokolov PAP, MS-CHAP, EAP-MD5, PEAP, EAP-Flexible, TEAP; • podpora autentifikácie cez tunel prostredníctvom protokolu FAST, TLS, TTLS.
Správa prístupov zariadení	• podpora protokolu TACACS+; • podpora prístupu používateľa na základe lokality, skupiny, prihlasovacích údajov;
Profilovanie zariadení	• podpora preddefinovaných šablón koncových zariadení ako sú IP telefóny, kamery, smartfóny, tablety, tlačiarne; • možnosť tvorby vlastných šablón zariadení pre potreby automatického zistenia, klasifikácie a priradenia identít pri pripájaní sa do siete; • možnosť priraďovania autorizačných politík špecifických pre koncový bod na základe identifikovaného typu zariadenia; • možnosť zberu údajov o atribútoch koncového bodu pomocou pasívneho monitorovania siete a telemetrie.
Hodnotenie zariadení pripojených do siete	• podpora vyhodnocovania koncových zariadení pripojených v sieti; • podpora vytvárania politík na kontrolu najnovších záplat OS, kontrolu aktuálnych verzií antivírusových a antispyware balíkov, kontrolu pravidiel šifrovania disku, prítomnosti aplikácií a pod. • podpora plnej viditeľnosti HW zariadení v sieti;
Podpora Active Directory	• podpora autentifikácie a autorizácie použitím multistromových Microsoft AD domén; • podpora grupovania viacerých nespojených domén do logických skupín; • možnosť flexibilného prepisovania pravidiel identít; • podpora Microsoft AD 2003, 2008, 2008R2, 2012, 2012R2, 2016 a 2019
Monitoring a riešenie problémov	• integrovaná konzola s webovým rozhraním pre účely monitorovania, generovania správ a riešenia problémov; • podporuje funkcionalitu záznamu všetkých aktivít a metrík v reálnom čase na úrovni všetkých používateľov a koncových bodov, ktoré sú pripojené v sieti.
Spôsob nasadenia	• možnosť nasadenia v prostredí verejného obstarávateľa v režime vysokej dostupnosti „HA". Prostredie virtualizácie a výpočtové zdroje poskytne verejný obstarávateľ.

Switch TYP 1 (7ks)	
Porty	• 24 portov 10/100/1000 Ethernet PoE+
Uplink rozhrania	• 4 x 1G SPF uplink
CPU	• ARM v 7 800 MHz
PoE+ power budget	• 195 W
DRAM	• 512 MB
Flash pamäť	• 256 MB
Šírka pásma – forwarding	• 28 Gbps
Šírka pásma – switching	• 56 Gbps
Rýchlosť preposielania (64 byte L3 paketov)	• 41,67 Mpps
Unicast MAC adresy	• 16000
IPv4 unicast direct routes	• 542
IPv4 unicast indirect routes	• 256
IPv6 unicast direct routes	• 414
IPv6 inicast indirect routes	• 128
IPv4 multicast routes a IGMP skupiny	• 1024
IPv6 multicast skupiny	• 1024
Maximálny počet aktívnych VLAN	• 256
MTU-L3 paket	• 9198 bajtov
Jumbo ethernet rámce	• 10 240 bajtov

Dodávka aktívnych prvkov CORE časti siete

- bez zmeny sieťovej a bezpečnostnej architektúry, jedná sa o technologický upgrade.

Firewall CORE časť - TYP 1 (2 ks)	
GE RJ-45 porty	• 16 ks
GE RJ-45 porty – manažment HA	• 1 ks
GE SFP slot	• 8 ks
10 GE SFP+	• 2 ks
USB port	• 1 ks
Konzolový port	• 1 ks
Vnútorné úložisko	• 480 GB SSD
IPS priepustnosť	• 5 Gbps
NGFW priepustnosť	• 3.5 Gbps
Ochrana pred hrozbami – priepustnosť	• 3 Gbps
UPv4 priepustnosť firewallu (1518 / 512 / 64 bajtov, UDP)	• 27 / 27 / 11 Gbps
Priepustnosť firewallu (paket / sekunda)	• 16.5 Mpps
Počet súčasných spojení (TCP)	• 3 000 000
Počet nových spojení TCP / sekunda	• 280 000
Počet politik FW	• 10 000
Priepustnosť IPsec VPN (256 bajtov)	• 13 Gbps
Počet GW to GW IPsec VPN tunelov	• 2 000
Počet klient – klient IPsec VPN tunelov	• 16 000
Priepustnosť SSL-VPN	• 2 Gbps
Počet súčasných SSL-VPN používateľov	• 500
Priepustnosť SSL inšpekcie	• 4 000 Gbps
SSL inšpekcia CPS	• 3 500
Počet súčasných spojení SSL inšpekcia	• 300 000
Priepustnosť kontroly aplikácií	• 13 Gbps
CAPWAP priepustnosť	• 20 Gbps
Počet virtuálnych domén	• 10
HA konfigurácia	• active-active, active-passive, clustering

Switch CORE časť - TYP 1 (2 ks)	
10/100/1000 porty	• 24x 1G SFP
Pamäť DRAM	• 8 GB
Pamäť flash	• 16 GB
Počet VLAN IDs	• 4094
Uplink konfigurácia	• Modulárna
Kapacita prepínania	• 208 Gbps
Prepínacia kapacita vrátane stackovania	• 688 Gbps
Rýchlosť preposielania	• 154,76 Mpps
Celový počet MAC adries	• 32 000
IPv4 direct routes	• 24 000
IPv4 indirect routes	• 8 000
IPv6 routes	• 16 000
Rozsah multicast routing	• 8 000
Rozsah QoS záznamov	• 5 120
Rozsah ACL záznamov	• 5 120
Jumbo ethernet rámce	• 9198 bajtov
Príslušenstvo – stohovací kábel 1	• 2x stohovací kábel; • Kompatibilný so Switch CORE TYP 1; • Dĺžka 0,5 m.
Príslušenstvo – stohovací kábel 2	• 2ks stohovací kábel; • Kompatibilný so Switch CORE TYP 1; • Možnosť sériového napájania zariadení; • Dĺžka 1,5 m.

Príslušenstvo – sieťový modul	• 10 GE SFP+; • Rýchlosť 1G/10Gb/s; • Chladenie pasívne; • Kompatibilita so Switch CORE TYP1.
Príslušenstvo – napájací zdroj	• redundantný napájací zdroj – dva zdroje; • Kompatibilný so Switch CORE TYP 1; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 715 W.
Príslušenstvo – SFP+ modul	• 12 ks SPF+ modul; • Kompatibilita so Switch CORE TYP1.

Switch CORE časť - TYP 2 (2 ks)	
10/100/1000 porty	• 24x 1G metalické
Pamäť DRAM	• 8 GB
Pamäť flash	• 16 GB
Počet VLAN IDs	• 4094
Uplink konfigurácia	• Modulárna
Kapacita prepínania	• 208 Gbps
Prepínacia kapacita vrátane stackovania	• 688 Gbps
Rýchlosť preposielania	• 154,76 Mpps
Celový počet MAC adries	• 32 000
IPv4 direct routes	• 24 000
IPv4 indirect routes	• 8 000
IPv6 routes	• 16 000
Rozsah multicast routing	• 8 000
Rozsah QoS záznamov	• 5 120
Rozsah ACL záznamov	• 5 120
Jumbo ethernet rámce	• 9198 bajtov
Príslušenstvo – stohovací kábel 2	• 2ks stohovací kábel; • Kompatibilný so Switch CORE TYP 2; • Možnosť sériového napájania zariadení; • Dĺžka 1,5 m.
Príslušenstvo – sieťový modul	• 10 GE SFP+; • Rýchlosť 1G/10Gb/s; • Chladenie pasívne; • Kompatibilita so Switch CORE TYP2.
Príslušenstvo – napájací zdroj	• Redundantný napájací zdroj - dva zdroje; • Kompatibilný so Switch CORE TYP 2; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 350 W.

Switch CORE časť - TYP 3 (1 ks)	
10/100/1000 porty	• 24
Pamäť DRAM	• 2 GB
Pamäť flash	• 4 GB
Počet VLAN IDs	• 4096
Kapacita prepínania	• 128 Gbps
Stakovacia šírka pásma	• 80 Gbps
Rýchlosť preposielania	• 95,23 Mpps
Celkový počet MAC adries	• 16 000
IPv4 direct routes	• 8 000
IPv4 indirect routes	• 3 000
IPv6 routes	• 1 500
Rozsah multicast routing	• 1 000
Rozsah QoS záznamov	• 1 000
Rozsah ACL záznamov	• 1 500
Jumbo ethernet rámce	• 9 198 bajtov
Príslušenstvo – napájací zdroj	• redundantný napájací zdroj – dva zdroje; • Kompatibilný so Switch CORE TYP 3; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 125 W.

Router CORE časť - TYP 1 (2 ks)	
10/100/1000 porty	• 24x 1G SFP
Pamäť DRAM	• 4 GB
Pamäť flash	• 2 GB
Ethernet LAN	• Áno
Podpora L2 VPN	• Áno
Podpora L3 VPN	• Áno
Rýchlosť prenosu	• 1 000, 10 000 Mbit/s
Podpora QoS	• Áno
Príslušenstvo – SFP+ modul	• 2 ks SPF+ modul; • Kompatibilita so Router časť CORE TYP1.

Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

Autentifikátor

- Počet užívateľov: 700;
- Počet mobilných SW tokenov: 650;
- Počet HW tokenov: 50;
- Počet užívateľských certifikátov: 700;
- Nasadenie vo VM úspešného poskytovateľa;
- Podpora hypervízorov: VMware ESXi/ ESX 6ú7/8, Microsoft Hyper-V Server 2010, 2012 RC a 2016, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV, Oracle OCI, Alibaba Cloud;
- Podpora režimu vysokej dostupnosti („HA");
- Možnosť upgrade licencie min. na dvojnásobok voči požadovanej kapacite;

Mobilný SW token / HW token

- V prípade SW tokenu, mobilná aplikácia kompatibilná s mobilnými zariadeniami iOS, Android, Windows;
- V prípade HW tokenu – prenosné zariadenie napr. vo forme kľúčenky.
- Požadovaný počet licencií pre koncové zariadenia: 700;
- inštalácia na mobilné zariadenia Verejného obstarávateľa (v prípade SW tokenu);
- funkcionalita generovania jednorazového hesla;
- dynamické generovanie hesiel;
- kompatibilita s ponúknutým VPN klientom a jestvujúcou infraštruktúrou Verejného obstarávateľa;
- overovanie užívateľov musí služba zabezpečovať prostredníctvom samostatného autentifikačného servera;
- podpora time-based ako aj event-based tokenov;
- kompatibilita s OATH.

VPN KLIENT

- Počet užívateľov: 700;
- Inštalácia na zariadenia Verejného obstarávateľa;
- Možnosť konfigurácie zero trust pravidiel prístupu do siete;
- Možnosť centrálneho manažmentu;
- Centralizované logovanie a reporting;
- Podpora IPSEC VPN a SSL VPN s viacfatorovým overením (podpora mobilného SW tokenu – kompatibilita s navrhovaným riešením Uchádzača);
- Podpora webfilteringu;
- Podpora výrobcu 24/7;
- On premise inštalácia;
- Jednoduché a prehľadné užívateľské prostredie;
- Podpora integrácie na Active Directory;
- Dynamické riadenie prístupu;
- Podpora užívateľských skupín;
- Podpora dynamickej voľby brány.

Manažment koncových zariadení

- Funkcionalita manažmentu koncových zariadení;
- Požaduje sa nasadenie v infraštruktúre dodávateľa;
- Podpora vzdialenej správy VPN klientov;
- Možnosť priraďovania bezpečnostných profilov pre skupiny koncových zariadení;
- podpora nasadzovania VPN klientov;
- správa aktualizácií a verzií VPN klientov;
- užívateľský dashboard;
- možnosť integrácie na Active Directory;
- automatické generovanie definovaných alertov;
- centralizovaný provisioning užívateľov;
- možnosť centralizovaného update VPN klientov;
- možnosť centralizovanej správy užívateľských skupín;

- funkcionalita karantény koncových zariadení;
- automatizovaný monitoring koncových zariadení (verzie, OS IP/MAC adresy, stav koncových zariadení).

Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

Platforma pre centralizovanú ochranu a správu 700 ks koncových staníc	
Centrálna správa a manažment koncových zariadení	• jednoduché používateľské grafické rozhranie centralizovaného manažmentu; • možnosť diaľkového nasadenia klientov na koncové zariadenia; • údaje o prevádzke na koncovej stanici zobrazované v reálnom čase; • integrácia na Active Directory; • centrálna správa karantény; • možnosť priraďovania koncových zariadení do skupín; • automatizované notifikácie; • centralizovaný provisioning klientov; • automatické reakcie systému na hrozby; • možnosť centralizovaného SW na koncovej stanici; • ochrana SSL VPN klienta;
Telemetria a monitoring koncových zariadení	• informácie a klientovi na koncovej stanici (verzia, OS, IP/MAX adresa, profil užívateľa); • stav klientskej stanice; • možnosť reportovania telemetrie na úrovni centrálnej správy;
Kompatibilita riešenia pre koncové stanice	• MS Windows, MacOS, iOS, Linux.

5.1 Prehľad e-Government komponentov

n/a

6. LEGISLATÍVA

Na dosiahnutie cieľov projektu nie je potrebná zmena legislatívy.

Projekt má za účel zosúladiť existujúci stav s právnymi predpismi:

- smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach, na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii – smernica NIS2,
- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o kybernetickej bezpečnosti"),
- Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
- Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 401/2003 Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy

7. ROZPOČET A PRÍNOSY

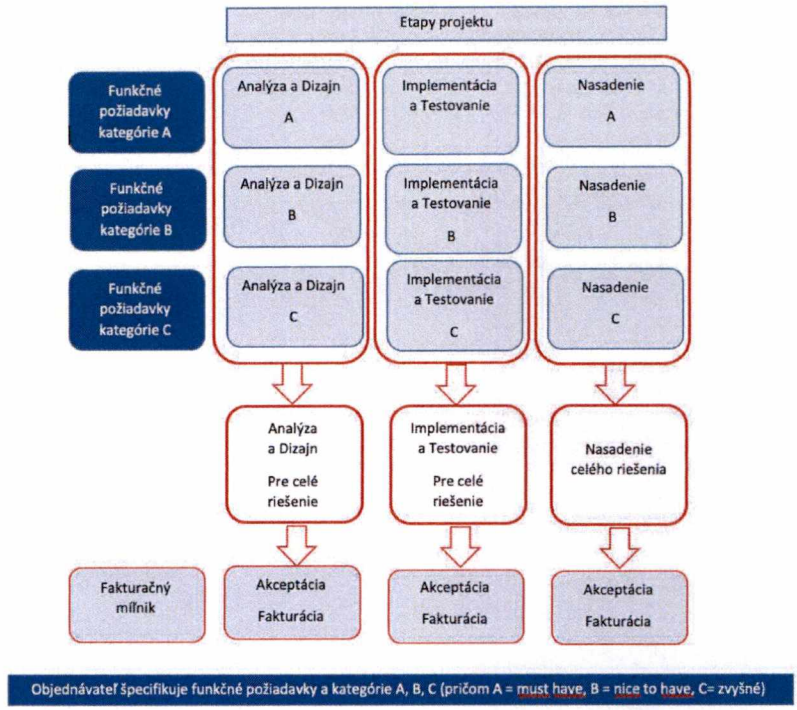
7.1 Sumarizácia nákladov a prínosov

Náklady (EUR s DPH)	**Modul: Audit bezpečnosti a hodnotenie rizík**	**Modul: Dokumentácia a politiky bezpečnosti**	**Modul : Správa prístupov koncových zariadení**	**Modul: Segmentácia siete a zabezpečenie komunikácie**	**Modul: Dodávka aktívnych prvkov siete**	**Modul: Dvojfaktorová autentifikácia**	**Modul: Centrálny bezpečnostný manažment**
Všeobecný materiál							
IT - CAPEX							
Aplikácie			*37.760,00*				*28.160,00*
SW						*31.632,00*	
HW			*8.372,00*		*121.164,00*	*2.498,00*	
Jednorazové činnosti expertov s dodaním diela	*8.500,00*	*60.360,00*	*18.340,00*	*36.404,00*	*18.340,00*	*11.160,00*	*11.200,00*

Náklady (EUR s DPH)	Modul: Audit bezpečnosti a hodnotenie rizík	Modul: Dokumentácia a politiky bezpečnosti	Modul : Správa prístupov koncových zariadení	Modul: Segmentácia siete a zabezpečenie komunikácie	Modul: Dodávka aktívnych prvkov siete	Modul: Dvojfaktorová autentifikácia	Modul: Centrálny bezpečnostný manažment
IT - OPEX- prevádzka							
Aplikácie							*1.465,00*
SW			*330,00*			*130,00*	
HW			*500,00*				
Prínosy							
Finančné prínosy							
Administratívne poplatky	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Ostatné daňové a nedaňové príjmy	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Ekonomické prínosy							
Občania (€)	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Úradníci (€)	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Úradníci (FTE)	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Kvalitatívne prínosy							

8. HARMONOGRAM JEDNOTLIVÝCH FÁZ PROJEKTU A METÓDA JEHO RIADENIA

ID	FÁZA/AKTIVITA	ZAČIATOK (odhad termínu)	KONIEC (odhad termínu)	POZNÁMKA
1.	*Prípravná fáza*	*02/2024*	*04/2024*	
2.	*Iniciačná fáza*	*08/2024*	*12/2024*	
3.	*Realizačná fáza*	*01/2025*	*12/2025*	
3a	*Analýza a dizajn*	*01/2025*	*03/2025*	
3b	*Nákup HW/SW*	*01/2025*	*12/2025*	
3c	*Implementácia a testovanie*	*04/2025*	*10/2025*	
3d	*Nasadenie*	*11/2025*	*12/2025*	
4.	*Dokončovacia*	*01/2026*	*02/2026*	
5.	*Podpora prevádzky SLA*	*03/2026*	*02/2031*	*5 rokov udržateľnosť (60 mesiacov)*



Pre tento projekt sa plánuje riadenie systémom „WATERFALL", ktorý sa javí ako vhodnejšia alternatíva k agilnému prístupu, nakoľko všetky projektové etapy bude pomerne jednoznačne možné identifikovať, ohraničiť a realizovať vo vzťahu k ich vecnej a časovej závislosti. V rámci ďalších fáz projektu, predovšetkým v Iniciačnej fáze budú bližšie špecifikované jednotlivé etapy projektu a súslednosť pracovných balíkov „WPs" a to v súlade s metodikou riadenia projektov PRINCE2.

Projekt bude teda nasledovať metódu Waterfall s dôkladnými logickými prepojeniami medzi jednotlivými modulmi, ktoré budú realizované na základe funkčnej a technickej špecifikácie pripravenej v rámci prípravy projektu. Tento rozhodnutý prístup vyplýva z potreby vykonávať opatrenia v kybernetickej bezpečnosti (KIB) v úzkej súvislosti, no v správnom poradí. Hoci niektoré aktivity môžu prebiehať súčasne a môžu byť vykonávané rôznymi tímami, dodržiavať budú predom stanovenú stratégiu a celkový plán projektu. Vzhľadom na potrebu realizácie projektu v kontinuálnej prevádzke základných služieb mesta, nie je vhodné zvoliť agilný prístup k realizácii tohto plánu.

9. PROJEKTOVÝ TÍM

Riadiaci výbor

Riadiaci výbor je orgán zriadený Mestom Banská Bystricia. Riadiaci výbor je najvyšší riadiaci a kontrolný orgán projektu. Riadiaci výbor tvorí predseda riadiaceho výboru a ostatní členovia. Riadiaci výbor sa riadi Štatútom Riadiaceho výboru, ktorý upravuje najmä jeho pôsobnosť, úlohy, zloženie, zasadnutie a hlasovanie. Členom riadiaceho výboru projektu môže byť aj zástupca dodávateľa. Väčšina členov riadiaceho výboru projektu s hlasovacím právom sú osoby navrhnuté Mestom zastupujú záujmy Mesta ako objednávateľa. Riadiaci výbor projektu dozerá na hospodárnosť, efektívnosť a účelové využívanie finančných prostriedkov a môže prispôsobiť štandardy projektového riadenia na realizovaný projekt.

Riadiaci výbor projektu tvoria minimálne 3 členovia, vrátane predsedu Riadiaceho výboru.

Riadiaci výbor (RV), v minimálnom zložení:

- predseda riadiaceho výboru,
- zástupca kľúčových používateľov objednávateľa,
- zástupca dodávateľa (doplní sa až po VO).

Riadiaci výbor je riadený predsedom, ktorým je zástupca Mesta Banská Bystrica. V prípade neprítomnosti predsedu na zasadnutí Riadiaceho výboru, predseda musí na toto konkrétne zasadnutie písomne delegovať svoju funkciu v rozsahu svojich práv a povinností formou splnomocnenia na zástupcu, ktorým môže byť aj iný člen Riadiaceho výboru s hlasovacím právom, prípadne iná splnomocnená osoba.

Riadiaci výbor zasadá pravidelne, najmenej jedenkrát za dva (2) po sebe nasledujúce kalendárne mesiace. Zasadnutie Riadiaceho výboru zvoláva predseda. Zasadnutie Riadiaceho výboru vedie predseda, prípadne ním určený zástupca, na ktorého predseda na dané zasadnutie písomne delegoval svoju funkciu, alebo ten člen Riadiaceho výboru, ktorý požiadal o zasadnutie Riadiaceho výboru.

Hlavné dokumenty spojené s činnosťou Riadiaceho výboru sú program zasadnutia, pracovný materiál a záznam zo zasadnutia Riadiaceho výboru, ktorého prílohou musí byť aj prezenčná listina, prípadne aj písomné splnomocnenia členov Riadiaceho výboru. Závery zo zasadnutia Riadiaceho výboru a jednotlivé body zo zasadnutia Riadiaceho výboru sa prijímajú súhlasným hlasovaním nadpolovičnej väčšiny prítomných členov Riadiaceho výboru s hlasovacím právom. Hlas predsedu má v prípade rovnosti hlasov hodnotu dvoch hlasov.

Každý člen Riadiaceho výboru ma tieto práva a povinnosti:

a) právo a povinnosť zúčastňovať sa na zasadnutiach Riadiaceho výboru,
b) právo uplatniť si pripomienky, podávať podnety alebo vyjadriť sa k pracovnému materiálu predloženému na zasadnutí Riadiaceho výboru alebo v rámci dištančného hlasovania, ak sa jedná o člena Riadiaceho výboru s hlasovacím právom,
c) právo podávať návrhy a podnety týkajúce sa činnosti Riadiaceho výboru,
d) právo nahliadať do projektovej dokumentácie,
e) navrhovať zmeny Štatútu,
f) iné práva v zmysle tohto Štatútu a Projektového iniciálneho dokumentu (PID).

Člen Riadiaceho výboru zachováva mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedel pri výkone svojej funkcie alebo v súvislosti s ňou a ktoré v záujme Riadiaceho výboru nemožno oznamovať tretím osobám, a to aj po ukončení realizácie projektu.

Riadiaci výbor sa zriaďuje na účely realizácie projektu a bude zostavený v zložení:

ID	Meno a Priezvisko	Pozícia	Subjekt
1.	TBD	Predseda RV	Mesto Banská Bystrica
3.	TBD	Kľúčový používateľ	Mesto Banská Bystrica
7.	TBD	Zástupca Zhotoviteľa	TBD

Podrobná štruktúra RVP bude definovaná v rámci projektového iniciálneho dokumentu („PID") v súlade s metodikou riadenia projektov PRINCE2®.

Projektový tím

Riadenie projektu zo strany Objednávateľa bude zabezpečené prostredníctvom Projektového manažéra a Finančného manažéra a bude trvať počas celej doby realizácie projektu. Bude pokrývať oblasť projektového riadenia (projektový manažment, celková koordinácia projektu, celkový dohľad nad dodávkou dodávaného Diela, vrátane kvality), finančného riadenia a monitorovania realizácie projektu v zmysle riadenia podľa Vyhlášky č. 401/2022 Z. z. v platnom znení.

Projektový tím bude pozostávať z pozícií:

i) Povinné projektové role:

- Projektový manažér objednávateľa;
- Kľúčový používateľ;
- IT architekt;
- Vlastník procesov;
- Manažér kybernetickej a informačnej bezpečnosti;
- Projektový manažér zhotoviteľa;
- Špecialista pre bezpečnosť IT;
- IT analytik;
- Špecialista pre infraštruktúrny/HW špecialista;
- IT/IS konzultant;
- IT tester;
- Školiteľ pre IT systémy.

iii) Ďalšie projektové role:

- Finančný manažér,

Projektový manažér Objednávateľa bude zabezpečovať koordináciu projektových činností a manažment v súlade s metodikou PRINCE2 (hlavné dokumenty, priebežné manažérske výstupy, a pod.). Projektový manažér Objednávateľa bude riadiť, administratívne a organizačne zabezpečovať implementáciu projektu, komunikovať s dodávateľmi, sledovať plnenie harmonogramu projektu a zabezpečovať dokumenty požadované MIRRI. Zároveň bude v spolupráci s projektovým manažérom dodávateľa koordinovať realizáciu hlavných aktivít, činností a úloh projektu. Zodpovednosťou projektového manažéra je v spolupráci s finančným manažérom (objednávateľa) finančné riadenie projektu kontrolu rozpočtu projektu a jeho súlad s účtovnými dokladmi. Kontrolu podpornej účtovnej dokumentácie a poradenstvo pri definovaní oprávnených výdavkov bude zabezpečovať finančný manažér Objednávateľa.

Súčasťou projektovej kancelárie a projektového riadenia bude tiež operatívna projektová podpora zabezpečujúca administratívnu podporu pre písomnú komunikáciu, administratívne vedenie projektovej dokumentácie a prípravu podkladov pre členov projektového tímu, organizáciu stretnutí a pod.. V rámci aktivity budú taktiež zabezpečovaný manažment a hodnotenie kvality zo strany Objednávateľa.

ID	Meno a Priezvisko	Pozícia	Organizačný útvar	Rola v projekte
1.	TBD	TBD	TBD	Projektový manažér
2.	TBD	TBD	TBD	Kľúčový používateľ
3.	TBD	TBD	TBD	IT architekt
4.	TBD	TBD	TBD	Vlastník procesov
5.	Ing. Bibiána Palušková	Manažér IB a KB	PR-MKB	Manažér kybernetickej a informačnej bezpečnosti
6.	TBD	TBD	TBD	Projektový manažér zhotoviteľa
7.	TBD	TBD	TBD	Špecialista pre bezpečnosť IT
8.	TBD	TBD	TBD	IT analytik
9.	TBD	TBD	TBD	Manažér kvality
10.	TBD	TBD	TBD	IT/IS konzultant
11.	TBD	TBD	TBD	IT tester
12.	TBD	TBD	TBD	Školiteľ pre IT systémy
13.	TBD	TBD	TBD	Finančný manažér

10. ODKAZY

n/a

11. PRÍLOHY

Príloha 1: Zoznam rizík a závislosti
Príloha 2: Katalóg požiadaviek

PRÍSTUP K PROJEKTU

Vzor pre manažérsky výstup I-03

podľa vyhlášky MIRRI č. 401/2023 Z. z.

Povinná osoba	Mesto Banská Bystrica
Názov projektu	Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica
Zodpovedná osoba za projekt	Ing. Beáta Galková
Realizátor projektu	Mesto Banská Bystrica
Vlastník projektu	Ing. Bibiána Palušková

Schvaľovanie dokumentu

Položka	**Meno a priezvisko**	**Organizácia**	**Pracovná pozícia**	**Dátum**	**Podpis** (alebo elektronický súhlas)
Vypracoval	Ing. Beáta Galková Ing. Bibiána Palušková	Mesto Banská Bystrica	Referent	22.04.2024	

1. HISTÓRIA DOKUMENTU

Verzia	**Dátum**	**Zmeny**	**Meno**
0.1	03.04.2024	Draft pracovnej verzie	Ing. Beáta Galková
0.2	22.04.2024	Zapracované pripomienky z v 0.1	Ing. Beáta Galková

2. ÚČEL DOKUMENTU

Tento dokument slúži pre účely prípravnej fázy projektu **„Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v Meste Banská Bystrica"**. Dokument sumarizuje, analyzuje a ďalej rozpracúva informácie z pohľadu aktuálneho stavu do takej úrovne detailu, aby bolo možné rozhodnúť o pokračovaní prípravy projektu, alokovaní rozpočtových zdrojov, personálnych kapacít a kvalifikovane rozhodnúť o prechode do iniciačnej fázy projektu.

Dokument súčasne rámcovo popisuje spôsob riešenia formou jednotlivých vrstiev architektúry, ktoré sú s ohľadom na charakter projektového zámeru relevantnými. Dokument sa podrobne nevenuje popisu business procesov, popisu dátovej a aplikačnej architektúry, nakoľko realizáciou projektu sa **neočakáva vykonať zásah do týchto domén architektúr modelu „ADM" podnikovej architektúry definovanej rámcom TOGAF®.**

Dokument súčasne zachytáva aspekty bezpečnostnej architektúry v kontexte sieťovej architektúry, na ktorú budú mať navrhované oblasti a aktivity projektu najzásadnejší dopad.

2.1 Použité skratky a pojmy

SKRATKA/POJEM	**POPIS**
IB	Informačná bezpečnosť
KB	Kybernetická bezpečnosť
2FA	Dvojfaktorové overovanie
HW	Hardvér
IKT	Informačno-komunikačné technológie
ISVS	Informačný systém verejnej správy
Mesto	Mesto Banská Bystrica
RV	Riadiaci výbor
SLA	Service Level Agreement
SW	Softvér

VO	Verejné obstarávanie
Zákon o KB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

2.2 Konvencie pre typy požiadaviek

Užívateľské požiadavky majú nasledovnú konvenciu:

U_nn_Rxx

- U – užívateľská požiadavka
- Nn – typ používateľa
- R – označenie požiadavky
- Xx – číslo požiadavky

Procesné požiadavky majú nasledovnú konvenciu:

P_ABXY_Rxx

- P - procesná požiadavka
- AB – označenie procesu
- XY – číslo podprocesu
- R – označenie požiadavky
- Xx – číslo požiadavky

Požiadavky na reporting majú nasledovnú konvenciu:

R_ABXY_Rxx

- R – požiadavka na reporting
- Nn – číslo reportu
- R – označenie požiadavky
- Xx – číslo požiadavky

3. POPIS NAVRHOVANÉHO RIEŠENIA

Predkladané riešenie bolo navrhnuté na základe vykonanej analýzy možných alternatívnych riešení pri súčasnom zohľadnení aktuálneho stavu v oblasti IB a KB v Meste Banská Bystrica. Pre stanovenie navrhovaného riešenia boli vykonané nasledovné vzájomne súvisiace úkony.

- Identifikácia a analýza nevyhnutných riešených oblastí zvýšenia úrovne informačnej bezpečnosti a kybernetickej bezpečnosti na podklade vykonaného auditu KB a opakovaného auditu KB;
- Sumarizácia možných oblastí podporujúcich zvýšenie úrovne IB a KB v organizácii, určenie úrovne priority ich realizácie s ohľadom na potrebu, možné dopady v oblasti IB a KB ako aj odhadované finančné, technické, personálne nároky;
- Selekcia konečného optimálneho setu oblastí v rámci, ktorých je potrebné vykonať nevyhnutné aktivity pre zvýšenie úrovne IB a KB v Meste Banská Bystrica;
- Realizácia alternatív na úrovni business vrstvy s cieľom stanovenia preferovaného variantu realizácie projektu a teda definovanie konečného rozsahu projektového zámeru a navrhovaného riešenia (viac viď kapitola 3.8 dokumentu „Projektový zámer").

Projekt v kontexte horeuvedeného postupu navrhuje s cieľom zaistenia kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB riešiť oblasti IB a KB, ktoré priamo reflektujú na známe zistenia z už vykonaných auditov KB realizovaných v prostredí organizácie, tak aby projekt v čo najväčšej možnej miere prispel k zosúladeniu oblasti riadenia kybernetickej a informačnej bezpečnosti s požiadavkami a očakávaniami príslušných štátnych orgánov ako aj príslušných aktuálne platných legislatívnych požiadaviek. **Projekt realizácie opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v Meste Banská Bystrica je zameraný na dobudovanie infraštruktúry, posilnenie kybernetickej bezpečnosti organizácie, zlepšenie procesov, komunikácie ako aj celkové uchytenie a zlepšenie úrovne governance v oblasti IB a KB v organizácii, zber a analýzu prevádzkových dát v sieti pre zamedzenie a/alebo efektívne riešenie prípadných bezpečnostných incidentov, zrýchlenie detekcie ako aj riešenia kybernetických incidentov pri ambícií posilnenia preventívnych opatrení nad následným incident/problem managementom.**

Iniciatíva projektu vychádza z viacerých základných predpokladov, ktoré sú vzájomne previazané:

- Nárast rizika kybernetických útokov zameraných na subjekty verejnej správy a prevádzkovateľov základnej služby;
- Potreba zvýšenia efektivity procesov riadenia informačnej a kybernetickej bezpečnosti rámci IKT organizácie;
- Potreba riešenia nedostatku kvalifikovaných odborných IKT špecialistov a špecialistov informačnej bezpečnosti a kybernetickej bezpečnosti prostredníctvom centrálnej správy, automatizácie a manažmentu procesov a aktív;
- Potreba zvýšenia transparentnosti a efektívnosti manažmentu výkonu prevádzky IKT v organizácii;
- Potreba zvýšenia visibility v monitorovaných IS prostredníctvom implementácie manažmentových a dohľadových nástrojov;
- Naplnenie zákonných a regulatívnych požiadaviek;
- Zvýšiť bezpečnosť siete prostredníctvom rozšírenia prístupových pravidiel pri zachovaní užívateľského komfortu;
- Absencia vykonania inventarizácie informačných aktív, vykonania klasifikácie a kategorizácie IS a sietí, vykonania AR a BIA ako aj absencia zabezpečenia formalizovaného a opakovaného procesu riadenia identifikovaných rizík (ich mitigácie), ktoré sú nevyhnutným a nutným predpokladom pre efektívne riadenie rizík IB a KB;
- Absencia bezpečnostných opatrení pre jednotlivé klasifikačné stupne a kategórie IS a absencia základnej sady dokumentácie požadovanej Zákonom o KB;
- Absencia základných smerníc pre výkon procesov riadenia IB a KB v rámci jednotlivých oblastí riadenia;
- Absencia ľudských kapacít na efektívny bezpečnostný monitoring, konsolidáciu logov a auditných záznamov, analýzu bezpečnostných udalostí a incidentov a aj na ich riešenie so súčasnou snahou odbúrania pracovnej záťaže prechodom na automatizáciu a digitalizáciu týchto procesov.

Hlavný cieľom projektu je **zaistenie kybernetickej ochrany v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona o KB.** Pre naplnenie cieľov boli identifikované nasledovné aktivity, ktoré bude potrebné vykonať:

1. Vykonať opakovaný audit informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB;
2. Vypracovať relevantnú bezpečnostnú dokumentáciu;
3. Implementovať a konfigurovať systém pre riadenie správy prístupov koncových zariadení do siete Mesta Banská Bystrica;
4. Vykonať segmentáciu siete Mesta Banská Bystrica s ohľadom na súčasné prevádzkové požiadavky;
5. Zrealizovať výmenu aktívnych prvkov CORE časti siete;
6. Implementovať systém dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete;
7. Implementovať riešenie centrálneho bezpečnostného manažmentu pre koncové stanice.

Paralelne s týmito aktivitami bude nevyhnutne potrebné v relevantných oblastiach vykonať školenia dotknutých stakeholderov na výstupy jednotlivých aktivít tak, aby bola zachovaná vysoká úroveň profesionality ako aj kontinuity prevádzky celého predmetu projektu.

Implementácia horeuvedených aktivít prispeje k celkovému zvýšeniu úrovne IB a KB v Meste Banská Bystrica a ako aj odstráneniu identifikovaných nesúladov, ktoré boli identifikované počas vykonaných auditov IB a KB. Súčasne sa od projektu očakáva prínos v oblasti zrýchlenia, identifikácie, analýzy hrozieb ako aj odstraňovania prípadných kybernetických incidentov. Projekt ako taký plne korešponduje so strategickým smerovaním Mesta Banská Bystrica v oblasti IB, KB a rozvoja IKT ako aj so strategickými dokumentami na národnej ako aj nadnárodnej úrovni, súlad s ktorými bol rovnako jedným z motivátorom realizácie projektu (viď kap 3 dokumentu Projektový zámer).

Popis navrhovaného riešenia/aktivít projektu

a. Vykonanie opakovaného auditu informačnej a kybernetickej bezpečnosti v súlade s § 29 Zákona o KB

Mesto Banská Bystrica v čase po vyhlásení výzvy: „Podpora v oblasti kybernetickej a informačnej bezpečnosti na regionálnej úrovni – verejná správa", kód: PSK-MIRRI-611-2024-DV-EFRR zahájilo plánovaný opakovaný audit kybernetickej bezpečnosti v súlade s § 29 Zákona o KB. Audit KB prebieha v čase 04/2024 pričom už z jeho priebehu je známe potvrdenie zistených nesúladov v audite vykonávanom v predchádzajúcom období. Ambíciou Mesta Banská Bystrica je využiť jestvujúce auditné správy ako aj predbežné informácie a konzultácie z prebiehajúceho auditu na adresnejšie a účelnejšie definovanie priorít a potrieb v oblasti zabezpečenia vysokej úrovne zabezpečenia IB a KB na úrovni celej organizácie. Identifikované riziká a slabé miesta boli pri selekcii a prioritizácii navrhovaných aktivít kľúčovým vstupom pre celé uchopenie projektového zámeru s ohľadom na možné dopady v oblasti IB a KB ako aj s ohľadom na efektívnu alokáciu limitovaných finančných, technických a personálnych kapacít v kontexte najväčšej možnej dosiahnutej protihodnoty ako aj súladu s legislatívou v oblasti IB a KB. Bez pravidelnej aktualizácie stavu zabezpečenia IB a KB v organizácii by Mesto Banská Bystrica na jednej strane nespĺňala požiadavky zo Zákona o KB, ktoré sa kladú na prevádzkovateľa základnej služby a súčasne by nebolo možné poznať efektívne možnosti a spôsoby dosiahnutia vyššej úrovne zabezpečenia IB a KB ako aj úrovne governance v oblasti IB a KB. V neposlednom rade je vykonanie opakovaného auditu KB nevyhnutným predpokladom pre zlepšenie povedomia a vzdelávania o aspektoch IB a KB na úrovni celej organizácie a na úrovni dotknutých stakeholderov. Táto aktivita je s ohľadom na uvedené vyššie vnímaná ako nevyhnutná prerekvizita pre ostatné časti súvisiaceho navrhovaného riešenia.

2. Vypracovanie relevantnej bezpečnostnej dokumentácie

Mesto Banská Bystrica v súčasnosti nedisponuje žiadnou z povinnej dokumentácie v zmysle Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných opatrení v znení vyhlášky č. 264/2023 Z.z. Z uvedeného dôvodu verejný obstarávateľ plánuje zabezpečiť vypracovanie relevantnej dokumentácie a zosúladenie so zákonnými požiadavkami kladenými na poskytovateľa základnej služby. V súčasnosti Mesto Banská Bystrica disponuje iba zriadeným bezpečnostným výborom, ale samotné riadenie informačnej bezpečnosti a kybernetickej bezpečnosti nie je vôbec formalizované. Predmetom zamýšľanej aktivity je vykonanie analýzy rizík („AR") pre aktíva podporujúce základnú službu podľa štandardov medzinárodnej normy ISO/IEC 27005:2018 a metodiky uvedenej vo Vyhláške NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení („Vyhláška o KB"). Súčasne sa plánuje v rámci uvedenej aktivity vykonať analýzu dopadov kľúčových činností a vyhodnotenie ich parametrov ako aj pripraviť základné politiky riadenia kybernetickej bezpečnosti podľa Zákona o KB a Vyhlášky o KB. Zároveň je v pláne vypracovať dokumentáciu relevantnú pre oblasť riadenia kontinuity činností a procesov, súčasne s vypracovaním a otestovaním týchto plánov v podmienkach organizácie.

V rámci aktivity sa plánuje dodanie nasledovnej bezpečnostnej dokumentácie, ktorá bude vychádzať z aktuálneho stavu informačnej a kybernetickej bezpečnosti ako aj aktuálne platného legislatívneho rámca:

- Vykonanie inventarizácie aktív vrátane klasifikácie informácií a kategorizácie sietí a informačných systémov;
- Vypracovanie analýzy rizík („AR") podľa požiadaviek uvedených vo Vyhláške o KB v súlade s metodikou medzinárodnej normy ISO/IEC 27005:2018. Aktivita bude súčasne zohľadňovať:
    - *relevantné hrozby;*
    - *aktíva podieľajúce sa na dodávke základnej služby;*
    - *relevantné a známe zraniteľnosti;*
    - *určenie pravdepodobnosti a odhad dopadov pri realizáciách hrozieb;*
    - *Stanovenie úrovne rizika;*
    - *Stanovenie miery účinkov bezpečnostných opatrení a úroveň reziduálneho rizika;*
    - *návrh opatrení na zníženie reziduálnych rizík, ktoré sú vyššie ako akceptovateľná miera definovaná vedením organizácie verejného obstarávateľa.*
    - *Vypracovanie sumárneho prehľadu kybernetických rizík v prostredí Mesta Banská Bystrica spolu s návrhom opatrení na ich zníženie s cieľom dosiahnutia akceptovateľnej miery rizika.*
- Vypracovanie analýzy dopadov a kľúčových procesov a činností („BIA") zahrňujúcej analýzu biznis dopadov („BIA"), vrátane prípravy smernice/metodiky pre riadenie oblasti BCM, prípravy plánov BCM a plánov obnovy DRP vrátane testovania navrhnutých plánov s vybranými zamestnancami Mesta Banská Bystrica. Aktivita bude súčasne zohľadňovať:
    - *Určenie funkčných závislostí kľúčových procesov v prostredí Mesta Banská Bystrica a potrebných zdrojov pre udržanie kontinuity ich výkonu;*
    - *Určenie relevantných scenárov havárií;*
    - *určenie parametrov „cieľový čas obnovenia – Recovery Time Objective (RTO)" a „cieľový bod obnovenia – Recovery Point Objective (RPO)" pre jednotlivé kľúčové procesy;*
    - *Identifikácia kľúčových procesov, ich závislostí a parametrov potrebných pre návrh náhradných scenárov obnovy pri havárii.*
- Vypracovanie základných bezpečnostných politík KB podľa Prílohy č. 1 k Vyhláške o KB:
    - *Bezpečnostná stratégia kybernetickej bezpečnosti;*
    - *Politika organizácie bezpečnosti;*
    - *Politika pre riadenie bezpečnosti rizík;*
    - *Politika pre riadenie informačných aktív;*
    - *Pravidlá správania sa a dobrej praxe;*
    - *Politika pre riadenie dodávateľských vzťahov;*
    - *Politika pre riadenie vývoja a údržby v oblasti IKT;*
    - *Politika pre riadenie a prevádzku IKT;*
    - *Politika pre riadenie súladu;*
    - *Politika pre riadenie kontinuity procesov a činností.*

3. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta

Súčasťou tejto aktivity projektu bude nasadenie SW riešenia na centralizovanú autentifikáciu a autorizáciu pre rôzne typy používateľov a zariadení v sieti, správu politík prístupu na základe možnosti definície identít, rolí, zariadení, prípadne ďalších, správcom siete voliteľných atribútov. Riešenie umožní sledovať a revidovať prístupy používateľov do siete Mesta, správu prístupov do siete zariadeniami pristupujúcimi v režime BYOD („Bring Your Own Device") – zariadení, ktoré nie sú v správe a priamej kontrole IKT Mesta. Implementované riešenie zjednotí, zjednoduší a urýchli správu prístupov v rámci siete Mesta Banská Bystrica a to prostredníctvom implementácie štandardu IEEE 802.1X pre autentifikáciu a autorizáciu zariadení, ktoré budú nadväzovať spojenie so sieťou Mesta. Správa prístupových práv a politík sa plánuje realizovať na úrovni portov aktívnych sieťových prvkov. Súčasťou tejto bude dodávka aktívnych sieťových prvkov vrátane realizácie inštalačných a konfiguračných služieb, ktoré zabezpečia vytvorenie a možnosť prevádzky bezpečnostného protokolu IEEE 802.1X v prostredí siete verejného obstarávateľa.

4 . Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky

Mesto Banská Bystrica má ambíciu vykonať segmentáciu siete v kontexte analýzy siete, ktorú bude nevyhnutné za týmto účelom vykonať. Obsahom tejto aktivity bude plánovanie segmentácie v kontexte identifikovaných možných logických segmentov s ohľadom na topológiu siete, prevádzkované agendové IS, výstupy realizovanej inventarizácie aktív a klasifikácie informácií a kategorizácie ako aj bezpečnostné požiadavky a požiadavky na výkonnosť. Predmetom dodávky bude vykonané mapovanie siete s cieľom získania komplexného a presného obrazu o existujúcej sieti Mesta vrátane všetkých relevantných informačných aktív.

V rámci realizovanej aktivity bude vykonané rozdelenie rozsahov IP adries v rámci vytváraných segmentov, pričom pre každé aktívum budú pridelené IP adresy z definovaných rozsahov. V rámci plnenia budú v kontexte novo dodávaných sieťových prvkov prehodnotené fyzické segmenty siete a z nich vychádzajúce logické segmenty pomocou VLAN. V rámci tejto aktivity sa vykoná konfigurácia dotknutých zariadení (switche, routre, firewally) tak, aby nastavenia zodpovedali schválenému návrhu segmentácie prevádzkou IKT Mesta. Súčasťou tejto aktivity zároveň bude vypracovanie komplexnej dokumentácie zachytávajúce celý stav vykonanej segmentácie, vrátane otestovania a overenia funkcionality.

Horeuvedené činnosti budú vykonávané v rozsahu siete v ktorej je aktívne využívaných 85 switchov, 40 routerov, 2 firewally vrátane zariadení, ktoré sú predmetom dodávky v rámci tohto projektu.

5. Výmena aktívnych prvkov CORE časti siete

V rámci tejto aktivity sa plánuje obstarať nové, nepoužité, v originálnom obale zabalené aktívne prvky CORE časti siete. Výmena sa plánuje s ohľadom na potrebu nahradenia end-of-sales and end-of-support aktívnych prvkov, doplnenie jestvujúcich ako aj s ohľadom na potrebu zabezpečenia väčšej bezpečnosti prevádzky siete ako aj prenosovej kapacity siete ako reakciou na neustále rastúce požiadavky na prenos v sieti Mesta. Od výmeny potrebných aktívnych prvkov CORE časti siete sa očakáva zároveň zabezpečiť kontinuitu požadovanej úrovne IT aktív ako aj primerané doby odozvy informačných aktív prevádzkovaných v sieti Mesta. Výmena aktívnych prvkov CORE časti siete je potrebná aj s ohľadom na zámer Mesta implementovať systém pre riadenie správy a prístupov koncových zariadení do siete Mesta a zámerom implementovať protokol IEEE 802.1X. Súčasný stav CORE časti siete neumožňuje

plnohodnotné nasadenie IEEE 802.1X v rozsahu očakávanej segmentácie siete zahŕňajúcej okrem nových CORE aktívnych prvkov aj obstarané aktívne prvky v rámci aktivity 3. tohto projektu. Mesto plánuje obstarať celkovo 9 ks aktívnych prvkov CORE časti siete. Súčasťou dodávky nových, nepoužitých zariadení zabalených v originálnom balení, bude ich inštalácia, konfigurácia a uvedenie do prevádzky tak, aby mohli dodávané zariadenia byť zahrnuté do výkonu segmentácie siete ako aj nasadenia overovania podľa IEEE 802.1X.

Súčasťou aktivity bude implementácia riešenia zberu prevádzkových údajov z dodaných zariadení typu Firewall.

6. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

V rámci tejto aktivity sa očakáva implementovať riešenie pre vzdialený prístup do siete vrátane dodania a nasadenia mobilných SW ako aj HW tokenov a autentifikačného servera vyžadujúceho druhý stupeň overenia užívateľa prihlasujúceho sa do internej siete prostredníctvom implementácie služby 2-faktorového overovania („2FA") pre celkovo 700 používateľov pristupujúcich do siete Mesta.

Navrhuje sa, aby implementovaný autentifikačný server od užívateľa vyžadoval zadanie mena a hesla a následne po úspešnom zadaní prihlasovacej kombinácie vyžiadal zadanie jednorazového hesla, ktoré bude možné užívateľom generovať prostredníctvom dodaného hardvérového a softvérového tokenu kompatibilného s mobilnými zariadeniami iOS, Android a Windows, čím sa zabezpečí ďalšia úroveň zabezpečenia prístupu do siete Mesta z vonkajšieho prostredia.

Súčasťou aktivity bude dodávka VPN klientov s bezpečnostným modelom s nulovou dôverou, teda VPN klient, ktorý zároveň disponuje funkcionalitou kontroly koncového zariadenia voči nastaveným prístupovým politikám. VPN klient bude zároveň disponovať funkcionalitou karantény pripájajúcich sa koncových zariadení a umožní izolovať napadnuté koncové zariadenia od zvyšku siete, čím sa minimalizuje ohrozenie internej siete z podozrivého zdroja.

7. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

V rámci tejto aktivity sa plánuje implementovať ucelené riešenie prevencie a detekcie pred hrozbami z vonkajšieho prostredia. Riešenie bude zabezpečovať centrálnu správu ochrany koncových staníc, detekciu nevyžiadanej aktivity na koncových staniciach, funkcionalitu monitoringu prevádzky na koncových zariadeniach, skenovanie koncových zariadení ako aj funkcionalitu centrálneho nastavovania bezpečnostných pravidiel a politík pre koncové zariadenia. Riešenie umožní centrálne nastavovanie SW na koncových staniciach, nadobúdať informácie o telemetrii a prevádzke koncových staníc ako vykonávať reportovanie na úrovni koncových staníc.

Všetky aktivity vyššie budú podporované prierezovou aktivitou pozostávajúcou zo školení dotknutého personálu pre účely zachovania vysokej úrovne IB a KB ako aj kontinuity prevádzky informačných aktív Mesta.

Jednotlivé aktivity možno považovať za navzájom vecne, technicky, procesne súvisiace a ich realizácia bude nutná vo vzájomnom časovom priebehu, tak aby sa dosiahol maximálny efekt z ich súčasnej realizácie.

4. ARCHITEKTÚRA RIEŠENIA PROJEKTU

Predmetom projektu je predovšetkým nákup HW a SW prostriedkov, analytické činnosti sieťových špecialistov a špecialistov pre oblasť IB a KB. Zmena biznis architektúry, aplikačnej ako ani technologickej nebude realizovaná a aj aj vzhľadom na skutočnosť, že v predmetom projektu nie je plánované budovanie ISVS ako ani rozvoj žiadneho z jestvujúcich ISVS a ani migrácia do vládneho cloudu. Celkový prístup k architektúre ako aj popis sieťovej architektúry a jej logického zapojenia je popísaný bližšie kap. 5 dokumentu Projektový zámer. Mesto Banská Bystrica zároveň v tejto súvislosti uvádza a má za to, že nie je účelné uvádzať do verejne prístupného dokumentu ďalšie podrobnosti týkajúce sa infraštruktúry, na ktorej je prevádzkovaná základná služba ako aj ďalšie pre Mesto dôležité informačné aktíva, a z tohto dôvodu ďalšie, pre tento projekt nepožadované detaily, nesprístupňuje. Informácie v dokumente Projektový zámer sú zároveň uvedené v takej úrovni detailu, aby bolo orgánu vedenia jednoznačne možné verifikovať prioritné oblasti, do ktorých Mesto Banská Bystrica potrebuje realizovať nevyhnutné investície.

4.1 Biznis vrstva

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

4.2 Aplikačná vrstva

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

4.3 Dátová vrstva

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

4.4 Technologická vrstva

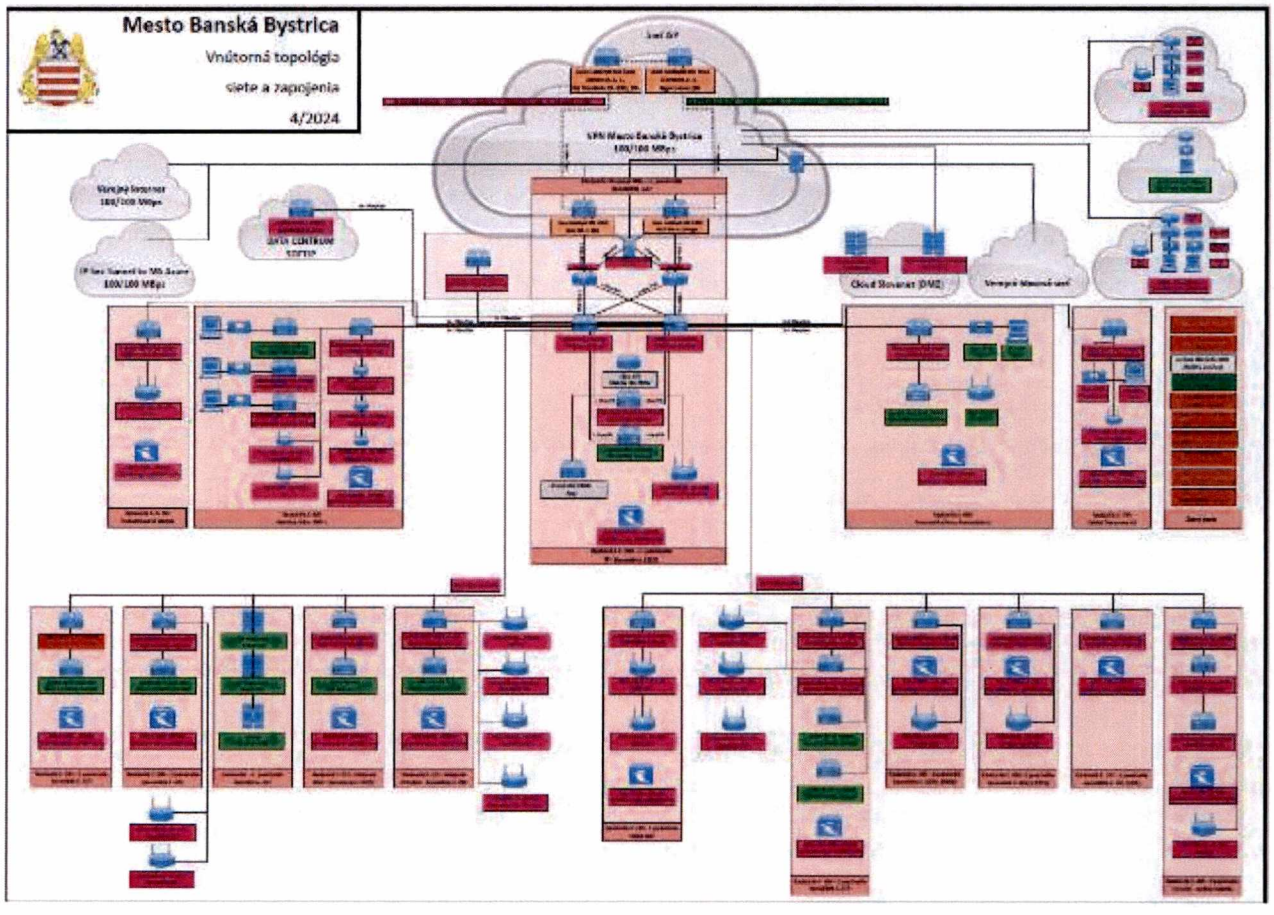
Súčasťou aktivít projektu je doplnenie jednotlivých HW položiek (firewally, router, switche) pre potreby obnovy jestvujúcej bezpečnostnej vrstvy. Položky, ktoré sa plánuje v rámci projektu nasadiť sú popísané vyššie v tomto dokumente ako aj v kap. 5 dokumentu Projektový zámer. Podrobná špecifikácia je obsiahnutá súčasne v rámci Výzvy na predkladanie indikatívnych cenových ponúk za účelom stanovenia predpokladanej nákladovosti hlavných aktivít projektu. Táto špecifikácia je zároveň v súlade s Katalógom požiadaviek, ktorý tvorí neoddeliteľnú súčasť dokumentácie k projektu.

4.4.1 Požiadavky na výkonnostné parametre, kapacitné požiadavky – TO BE

Parameter	Jednotky	Predpokladaná hodnota	Poznámka
Počet interných používateľov	Počet	250	Zamestnanci MsÚ
Počet súčasne pracujúcich interných používateľov v špičkovom zaťažení	Počet	700	Vrátane zamestnancov Mesta vrátane zamestnancov MsÚ
Počet externých používateľov (internet)	Počet	100 000	
Počet externých používateľov používajúcich systém v špičkovom zaťažení	Počet	125 000	
Počet transakcií (požiadavky na sieťový traffic)	Počet/obdobie	Viď Výzva Projektový zámer – špecifikácia HW	Požiadavky na aktívne sieťové prvky

4.4.2 Návrh riešenia technologickej / bezpečnostnej architektúry

Realizáciou aktivít projektu nedôjde k zmene topológie siete, ktorá v stave „AS-IS" zodpovedá schéme nižšie:



4.4.3 Využívanie služieb z katalógu služieb vládneho cloudu

Vzhľadom na charakter projektu sa nebudú využívať žiadne služby vládneho cloudu.

5. ZÁVISLOSTI NA OSTATNÉ ISVS / PROJEKTY

Neevidujú sa žiadne závislosti na iné projekty alebo ISVS.

6. ZDROJOVÉ KÓDY

Vzhľadom na charakter projektu – projekt z oblasti IB a KB je daná časť irelevantná.

7. PREVÁDZKA A ÚDRŽBA

7.1 Prevádzkové požiadavky

Prevádzkové požiadavky budú pre navrhované riešenie rovnaké ako je ich súčasná úroveň:

Úrovne podpory používateľov:

Help Desk bude realizovaný cez 3 úrovne podpory s nasledovným označením:

L1 podpora riešenia (LEVEL 1, priamy kontakt používateľa) – zabezpečuje prevádzka IKT Mesta;
L2 podpora riešenia (LEVEL 2, postúpenie požiadaviek od L1) – vybraná skupina garantov so základnou znalosťou riešenia, zabezpečuje Help Desk prvej úrovne dodávateľa riešenia. Úroveň služieb, rozsah ako aj reakčné časy budú závislé od definovanej úrovne SLA zmluvy;
L3 podpory riešenia (LEVEL 3, postúpenie požiadaviek od L2) – vybraná skupina garantov s vysokou úrovňou špecializácie na v riešení použité technológie a postupy, rozsah ako aj reakčné časy budú závislé od definovanej úrovne SLA zmluvy.

Definícia:

Podpora L1 (podpora 1. stupňa) – začiatočná úroveň podpory, ktorá je zodpovedná za riešenie základných problémov a požiadaviek koncových používateľov a ďalšie služby vyžadujúce základnú úroveň technickej podpory. Základnou úlohou podpory 1. stupňa je zhromaždiť informácie, vykonať základnú analýzu a určiť príčinu problému a jeho klasifikáciu. Typicky sú v tejto úrovni riešené priamočiare a jednoduché problémy a základné diagnostiky, overenie dostupnosti jednotlivých vrstiev infraštruktúry (sieťové, operačné, vizualizačné, aplikačné a pod...) a základné užívateľské problémy (napr. zabudnutie hesla), overovanie nastavení SW a HW a pod.

Podpora L2 (podpora 2. stupňa) – riešiteľské tímy s hlbšou technologickou znalosťou akou disponuje L1. Riešitelia na úrovni podpory L2 komunikujú s L1 úrovňou a sú zodpovední za poskytovanie súčinnosti tejto úrovni. L2 úroveň zodpovedá za poskytovanie súčinnosti úrovni L1 v prípade, že L1 úroveň eskaluje na L2 úroveň svoju požiadavku. L2 úroveň zabezpečuje hlbšiu úroveň analýzy problému ako aj technickejší pohľad na riešenie problému. Výstupom kontroly na úrovni L2 môže byť potvrdenie, upresnenie alebo prehodnotenie hlásenia v závislosti na potrebách Mesta. Primárnym cieľom na úrovni L2 je dostať hlásenie čo najskôr pod kontrolu a následne ho adekvátne vyriešiť, prípadne neodkladne eskalovať problém na L3 úroveň.

Podpora L3 (podpora 3. stupňa) – predstavuje najvyššiu úroveň podpory pre riešenie najkomplexnejších a najkomplikovanejších incidentov/problémov, vrátane prevádzania hĺbkových analýz a riešenie extrémnych prípadov.

Očakávaná úroveň SLA:

Služby pre zamestnancov úradu: 24/7/365 s možnosťou nahlasovania prostredníctvom call centra a/alebo dedikovaného rozhrania helpdesku s funkcionalitou ticketovacieho systému pre manažment incidentov ako aj meranie reakčných časov.

Riešenie incidentov – SLA parametre

Za incident je považovaná chyba v diele (riešení) t.j. správanie sa v rozpore s prevádzkovou a používateľskou dokumentáciou diela. Za incident nie je považovaná chyba, ktorá nastala mimo prostredia riešenia, napríklad výpadok el. energie, alebo vyššia moc, prípadne iná udalosť, ktorú nebolo možné dôvodným spôsobom predvídať.

Označovanie naliehavosti hlásených incidentov:

Označenie naliehavosti incidentu (kategória)	Závažnosť incidentu	Popis naliehavosti incidentu
A	Kritická	Je to vada spôsobená vážnou chybou a/alebo nedostatkom dodávaného riešenia, pričom táto chyba a/alebo nedostatok zabraňuje používaniu dodávaného riešenia. Nie je možné poskytnúť požadovaný výstup z riešenia.
B	Vysoká	Je vada, spôsobená chybou a/alebo nedostatkom dodávaného riešenia, pričom táto chyba a/alebo nedostatok obmedzuje používanie dodávaného riešenia nasledovne: Niektoré funkcie (moduly, komponenty, objekty, programy) dodávaného riešenia nie sú funkčné alebo nie je umožnený prístup k niektorej funkcii (modulu, komponentu, objektu, programu) dodávanej dodávaného riešenia.
C	Stredná	Do tejto kategórie spadajú všetky chyby a/alebo nedostatky spojené s používaním dodávaného riešenia, ktoré nie sú klasifikované ako závažné alebo kritické vady, pričom však čiastočne obmedzujú používanie dodávaného riešenia. Nastavenie parametrov systému Poskytovateľom alebo (ii) Vzniknutá vada a/alebo nedostatok má za príčinu miernu nepohodlnosť pri práci s dodávaným riešením, ktorá je však funkčná.

Úroveň možného dopadu

Označenie závažnosti incidentu	Dopad	Popis dopadu
1	Katastrofický	Katastrofický dopad, priamy finančný dopad alebo strata dát (napr. znefunkčnenie základnej služby v celom jej rozsahu).
2	Značný	Značný dopad alebo strata dát (napr. znefunkčnenie základnej služby v jej podstatnom rozsahu).
3	Malý	Malý dopad alebo strata dát (ostatné udalosti nespadajúce do kategórie značný alebo katastrofický).

Výpočet priority incidentu je kombináciou dopadu a naliehavosti v súlade s best practices ITIL V3 uvedený v nasledovnej matici:

Označenie priority incidentu	Reakčná doba[1] od nahlásenia incidentu po začiatok riešenia incidentu	Doba konečného vyriešenia incidentu od nahlásenia incidentu (DKVI)[2]	Spoľahlivosť [3] (počet incidentov za mesiac)
1	0,5 hod.	4 hodín	1
2	1 hod.	12 hodín	2
3	1 hod.	24 hodín	10
4	1 hod.	Vyriešené a nasadené v rámci plánovaných releasov	

(1) Reakčná doba je čas medzi nahlásením incidentu Mestom Banská Bystrica (vrátane užívateľov riešenia, ktorí nie sú v pracovnoprávnom vzťahu s Mestom) na helpdesk úrovne L2 a jeho prevzatím na riešenie.

(2) DKVI znamená obnovenie štandardnej prevádzky - čas medzi nahlásením incidentu Mestom Banská Bystrica a vyriešením incidentu úspešným uchádzačom (do doby, kedy je funkčnosť prostredia znovu obnovená v plnom rozsahu). Doba konečného vyriešenia incidentu od nahlásenia incidentu Mestom Banská Bystrica (DKVI) sa počíta počas celého dňa. Do tejto doby sa nezarátava čas potrebný na nevyhnutnú súčinnosť Mesta Banská Bystrica, ak je potrebná pre vyriešenie incidentu. V prípade potreby je úspešný uchádzač oprávnený požadovať od Mesta Banská Bystrica schválenie riešenia incidentu.

(3) Maximálny počet incidentov za kalendárny mesiac. Každá ďalšia chyba nad stanovený limit spoľahlivosti sa počíta ako začatý deň omeškania bez odstránenia vady alebo incidentu. Duplicitné alebo technicky súvisiace incidenty (zadané v rámci jedného pracovného dňa, počas pracovného času 8 hodín) sú považované ako jeden incident.

4) Incidenty nahlásené Mestom Banská Bystrica úspešnému uchádzačovi:

a. Majú prioritu 3 a nižšiu;

7.2 Požadovaná dostupnosť IS:

Popis	Parameter	Poznámka
Prevádzkové hodiny	8 hodín	od 8:00 hod. - do 16:00 hod. počas pracovných dní
Servisné okno	10 hodín	od 19:00 hod. - do 5:00 hod. počas pracovných dní
	24 hodín	od 00:00 hod. - 23:59 hod. počas dní pracovného pokoja a štátnych sviatkov Servis a údržba sa bude realizovať mimo pracovného času.
Dostupnosť produkčného prostredia IS	99,90 %	98,5% z 24/7/365 t.j. max ročný výpadok je 66 hod. Maximálny mesačný výpadok je 5,5 hodiny. Vždy sa za takúto dobu považuje čas od 0.00 hod. do 23.59 hod. počas pracovných dní v týždni. Nedostupnosť IS sa počíta od nahlásenia incidentu Zákazníkom v čase dostupnosti podpory Poskytovateľa (t.j. nahlásenie incidentu na L3 v čase od 6:00 hod. - do 18:00 hod. počas pracovných dní). Do dostupnosti IS nie sú započítavané servisné okná a plánované odstávky IS. V prípade nedodržania dostupnosti IS bude každý ďalší začatý pracovný deň nedostupnosti braný ako deň omeškania bez odstránenia vady alebo incidentu.

7.2.1 Dostupnosť (Availability)

Dostupnosť znamená, že riešenie ako výstup projektu je prístupné v okamihu jeho potreby. Narušenie dostupnosti sa označuje ako nežiaduce zničenie (destruction) alebo nedostupnosť. Dostupnosť je zvyčajne vyjadrená ako percento času v danom období, obvykle za rok. V projekte sa uvažuje 99,90 % dostupnosť.

7.2.2 RTO (Recovery Time Objective)

V rámci projektu sa očakáva obnova po výpadku do 4 hodín resp. v závislosti od závažnosti identifikovaného problému.

7.2.3 RPO (Recovery Point Objective)

Projekt nerieši zálohovanie dát – výpadok riešenia nebude mať dopad na jestvujúce ISVS a ich zálohovanie dát.

8. POŽIADAVKY NA PERSONÁL

Projekt sa bude riadiť v súlade s platnou legislatívou v oblasti riadenia projektov IT. Pre potreby riadenia projektu bude vytvorený riadiaci výbor projektu a budú menovaní členovia Riadiaceho výboru projektu (ďalej len „RV"), projektový manažér a členovia projektového tímu.

Riadiaci výbor projektu tvoria minimálne 3 členovia, vrátane predsedu Riadiaceho výboru.
Riadiaci výbor (RV), v minimálnom zložení:

- predseda riadiaceho výboru;
- zástupca kľúčových používateľov objednávateľa;
- zástupca dodávateľa (doplní sa až po VO).

Riadiaci výbor je riadený predsedom, ktorým je zástupca Mesta Banská Bystrica. V prípade neprítomnosti predsedu na zasadnutí Riadiaceho výboru, predseda musí na toto konkrétne zasadnutie písomne delegovať svoju funkciu v rozsahu svojich práv a povinností formou splnomocnenia na zástupcu, ktorým môže byť aj iný člen Riadiaceho výboru s hlasovacím právom, prípadne iná splnomocnená osoba.

Riadiaci výbor zasadá pravidelne, najmenej jedenkrát za dva (2) po sebe nasledujúce kalendárne mesiace. Zasadnutie Riadiaceho výboru zvoláva predseda. Zasadnutie Riadiaceho výboru vedie predseda, prípadne ním určený zástupca, na ktorého predseda na dané zasadnutie písomne delegoval svoju funkciu, alebo ten člen Riadiaceho výboru, ktorý požiadal o zasadnutie Riadiaceho výboru.

Hlavné dokumenty spojené s činnosťou Riadiaceho výboru sú program zasadnutia, pracovný materiál a záznam zo zasadnutia Riadiaceho výboru, ktorého prílohou musí byť aj prezenčná listina, prípadne aj písomné splnomocnenia členov Riadiaceho výboru. Závery zo zasadnutia Riadiaceho výboru a jednotlivé body zo zasadnutia Riadiaceho výboru sa prijímajú súhlasným hlasovaním nadpolovičnej väčšiny prítomných členov Riadiaceho výboru s hlasovacím právom. Hlas predsedu má v prípade rovnosti hlasov hodnotu dvoch hlasov.

Každý člen Riadiaceho výboru ma tieto práva a povinnosti:

a. právo a povinnosť zúčastňovať sa na zasadnutiach Riadiaceho výboru;
b. právo uplatniť si pripomienky, podávať podnety alebo vyjadriť sa k pracovnému materiálu predloženému na zasadnutí Riadiaceho výboru alebo v rámci dištančného hlasovania, ak sa jedná o člena Riadiaceho výboru s hlasovacím právom,
c. právo podávať návrhy a podnety týkajúce sa činnosti Riadiaceho výboru,
d. právo nahliadať do projektovej dokumentácie,
e. navrhovať zmeny Štatútu,
f. iné práva v zmysle tohto Štatútu a Projektového iniciálneho dokumentu (PID).

Člen Riadiaceho výboru zachováva mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedel pri výkone svojej funkcie alebo v súvislosti s ňou a ktoré v záujme Riadiaceho výboru nemožno oznamovať tretím osobám, a to aj po ukončení realizácie projektu. Riadiaci výbor sa zriaďuje na účely realizácie projektu a bude zostavený v zložení:

ID	Meno a Priezvisko	Pozícia	Subjekt
1.	TBD	Predseda RV	Mesto Banská Bystrica
3.	TBD	Kľúčový používateľ	Mesto Banská Bystrica
7.	TBD	Zástupca Zhotoviteľa	TBD

Podrobná štruktúra RVP bude definovaná v rámci projektového iniciálneho dokumentu („PID") v súlade s metodikou riadenia projektov PRINCE2®.

Projektový tím

Riadenie projektu zo strany Objednávateľa bude zabezpečené prostredníctvom Projektového manažéra a Finančného manažéra a bude trvať počas celej doby realizácie projektu. Bude pokrývať oblasť projektového riadenia (projektový manažment, celková koordinácia projektu, celkový dohľad nad dodávkou dodávaného Diela, vrátane kvality), finančného riadenia a monitorovania realizácie projektu v zmysle riadenia podľa Vyhlášky č. 401/2022 Z. z. v platnom znení.

Projektový tím bude pozostávať z pozícií:

Povinné projektové role:

- Projektový manažér objednávateľa;
- Kľúčový používateľ;
- IT architekt;
- Vlastník procesov;
- Manažér kybernetickej a informačnej bezpečnosti;
- Projektový manažér zhotoviteľa;
- Špecialista pre bezpečnosť IT;
- IT analytik;
- Špecialista pre infraštruktúrny/HW špecialista;
- IT/IS konzultant;
- IT tester;
- Školiteľ pre IT systémy.
- iii) Ďalšie projektové role:
- Finančný manažér,

Projektový manažér Objednávateľa bude zabezpečovať koordináciu projektových činností a manažment v súlade s metodikou PRINCE2 (hlavné dokumenty, priebežné manažérske výstupy, a pod.). Projektový manažér Objednávateľa bude riadiť, administratívne a organizačne zabezpečovať implementáciu projektu, komunikovať s dodávateľmi, sledovať plnenie harmonogramu projektu a zabezpečovať dokumenty požadované MIRRI. Zároveň bude v spolupráci s projektovým manažérom dodávateľa koordinovať realizáciu hlavných aktivít, činností a úloh projektu. Zodpovednosťou projektového manažéra je v spolupráci s finančným manažérom (objednávateľa) finančné riadenie projektu kontrolu rozpočtu projektu a jeho súlad s účtovnými dokladmi. Kontrolu podpornej účtovnej dokumentácie a poradenstvo pri definovaní oprávnených výdavkov bude zabezpečovať finančný manažér Objednávateľa.

Súčasťou projektovej kancelárie a projektového riadenia bude tiež operatívna projektová podpora zabezpečujúca administratívnu podporu pre písomnú komunikáciu, administratívne vedenie projektovej dokumentácie a prípravu podkladov pre členov projektového tímu, organizáciu stretnutí a pod.. V rámci aktivity budú taktiež zabezpečovaný manažment a hodnotenie kvality zo strany Objednávateľa.

ID	Meno a Priezvisko	Pozícia	Organizačný útvar	Rola v projekte
1.	TBD	TBD	TBD	Projektový manažér
2.	TBD	TBD	TBD	Kľúčový používateľ
3.	TBD	TBD	TBD	IT architekt
4.	TBD	TBD	TBD	Vlastník procesov
5.	Ing. Bibiána Palušková	Manažér IB a KB	PR-MKB	Manažér kybernetickej a informačnej bezpečnosti
6.	TBD	TBD	TBD	Projektový manažér zhotoviteľa
7.	TBD	TBD	TBD	Špecialista pre bezpečnosť IT
8.	TBD	TBD	TBD	IT analytik
9.	TBD	TBD	TBD	Manažér kvality
10.	TBD	TBD	TBD	IT/IS konzultant
11.	TBD	TBD	TBD	IT tester
12.	TBD	TBD	TBD	Školiteľ pre IT systémy
13.	TBD	TBD	TBD	Finančný manažér

9. IMPLEMENTÁCIA A PREBERANIE VÝSTUPOV PROJEKTU

Projekt bude v zmysle Vyhlášky 401/2023 Z.z. o riadení projektov a zmenových požiadaviek riadený a realizovaný spôsobom waterfall. Projekt bude vzhľadom na previazanosť jednotlivých aktivít realizovaný v rámci jedného samostatného inkrementu.

10. PRÍLOHY

Dokument neobsahuje žiadne prílohy.

Opis predmetu zákazky – Funkčná špecifikácia

Realizáciou tejto zákazky verejný obstarávateľ sleduje splnenie nasledovných cieľov:

- Zaistiť kybernetickú ochranu v podmienkach Mesta Banská Bystrica v súlade s ustanoveniami Zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov („Zákon o KB").

Uvedené plánuje Mesto Banská Bystrica zabezpečiť prostredníctvom realizácie nasledovných opatrení, ktoré prispejú k celkovému zlepšeniu technologického, procesného, infraštruktúrneho, vedomostného a organizačného zabezpečenia zručností a kapacít pre plnenie úloh v oblasti informačnej a kybernetickej bezpečnosti v prostredí Mesta:

1. Vypracovanie relevantnej bezpečnostnej dokumentácie;
2. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta;
3. Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky;
4. Dodávka aktívnych prvkov CORE časti siete;
5. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete;
6. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice.

Predmet zákazky

1. Vypracovanie relevantnej bezpečnostnej dokumentácie

Verejný obstarávateľ v súčasnosti nedisponuje žiadnou z povinnej dokumentácie v zmysle Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných opatrení v znení vyhlášky č. 264/2023 Z.z. Z uvedeného dôvodu verejný obstarávateľ požaduje zabezpečiť vypracovanie relevantnej dokumentácie a zosúladenie so zákonnými požiadavkami kladenými na poskytovateľa základnej služby. V súčasnosti Mesto Banská Bystrica disponuje iba zriadeným bezpečnostným výborom, ale samotné riadenie informačnej bezpečnosti a kybernetickej bezpečnosti nie je vôbec formalizované. Predmetom zákazky je vykonanie analýzy rizík („AR") pre aktíva podporujúce základnú službu podľa štandardov medzinárodnej normy ISO/IEC 27005:2018 a metodiky uvedenej vo Vyhláške NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení („Vyhláška o KB"). Súčasne verejný obstarávateľ požaduje vykonať analýzy dopadov kľúčových činností a vyhodnotenie ich parametrov ako aj pripraviť základné politiky riadenia kybernetickej bezpečnosti podľa Zákona o KB a Vyhlášky o KB. Verejný obstarávateľ súčasne požaduje vypracovať dokumentáciu relevantnú pre oblasť riadenia kontinuity činností a procesov, súčasne s vypracovaním a otestovaním týchto plánov v podmienkach verejného obstarávateľa.

Verejný obstarávateľ v rámci predmetu plnenia požaduje dodanie nasledovnej bezpečnostnej dokumentácie, ktorá bude vychádzať z aktuálneho stavu informačnej a kybernetickej bezpečnosti ako aj aktuálne platného legislatívneho rámca:

- Vykonanie inventarizácie aktív vrátane klasifikácie informácií a kategorizácie sietí a informačných systémov;
- Vypracovanie analýzy rizík („AR“) podľa požiadaviek uvedených vo Vyhláške o KB v súlade s metodikou medzinárodnej normy ISO/IEC 27005:2018. Aktivita bude súčasne zohľadňovať:
    - *relevantné hrozby;*
    - *aktíva podieľajúce sa na dodávke základnej služby;*
    - *relevantné a známe zraniteľnosti;*
    - *určenie pravdepodobnosti a odhad dopadov pri realizáciách hrozieb;*
    - *Stanovenie úrovne rizika;*
    - *Stanovenie miery účinkov bezpečnostných opatrení a úroveň reziduálneho rizika;*
    - *návrh opatrení na zníženie reziduálnych rizík, ktoré sú vyššie ako akceptovateľná miera definovaná vedením organizácie verejného obstarávateľa.*
    - *Vypracovanie sumárneho prehľadu kybernetických rizík v prostredí verejného obstarávateľa spolu s návrhom opatrení na ich zníženie s cieľom dosiahnutia akceptovateľnej miery rizika.*
- Vypracovanie analýzy dopadov a kľúčových procesov a činností („BIA“) zahrňujúcej analýzu biznis dopadov („BIA“), vrátane prípravy smernice/metodiky pre riadenie oblasti BCM, prípravy plánov BCM a plánov obnovy DRP vrátane testovania navrhnutých plánov s vybranými zamestnancami verejného obstarávateľa. Aktivita bude súčasne zohľadňovať:
    - *Určenie funkčných závislostí kľúčových procesov v prostredí verejného obstarávateľa a potrebných zdrojov pre udržanie kontinuity ich výkonu;*
    - *Určenie relevantných scenárov havárií;*
    - *určenie parametrov „cieľový čas obnovenia – Recovery Time Objective (RTO)“ a „cieľový bod obnovenia – Recovery Point Objective (RPO)“ pre jednotlivé kľúčové procesy;*
    - *Identifikácia kľúčových procesov, ich závislostí a parametrov potrebných pre návrh náhradných scenárov obnovy pri havárii.*
- Vypracovanie základných bezpečnostných politík KB podľa Prílohy č. 1 k Vyhláške o KB:
    - *Bezpečnostná stratégia kybernetickej bezpečnosti;*
    - *Politika organizácie bezpečnosti;*
    - *Politika pre riadenie bezpečnosti rizík;*
    - *Politika pre riadenie informačných aktív;*
    - *Pravidlá správania sa a dobrej praxe;*
    - *Politika pre riadenie dodávateľských vzťahov;*
    - *Politika pre riadenie vývoja a údržby v oblasti IKT;*
    - *Politika pre riadenie a prevádzku IKT;*
    - *Politika pre riadenie súladu;*
    - *Politika pre riadenie kontinuity procesov a činností.*

Plnenie bude pozostávať z poskytnutia služieb – činností expertov v oblasti IB a KB v nasledovnom rozsahu:

Názov pozície	**Merná jednotka (m.j.)**	**Počet m.j.**
Projektový manažér IT projektu	*Človekodeň (MD)*	*5*
IT analytik	*Človekodeň (MD)*	*35*

Špecialista pre bezpečnosť IT	*Človekodeň (MD)*	*10*
Špecialista pre infraštruktúrny/HW špecialista	*Človekodeň (MD)*	*5*
Špecialista pre databázy	*Človekodeň (MD)*	*5*
IT/IS konzultant	*Človekodeň (MD)*	*25*
SPOLU	**Človekodeň (MD)**	**85**

2. Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta

Súčasťou dodávky bude nasadenie SW riešenia na centralizovanú autentifikáciu a autorizáciu pre rôzne typy používateľov a zariadení v sieti, správu politík prístupu na základe možnosti definície identít, rolí, zariadení, prípadne ďalších, správcom siete voliteľných atribútov. Riešenie umožní sledovať a revidovať prístupy používateľov do siete verejného obstarávateľa, správu prístupov do siete zariadeniami pristupujúcimi v režime BYOD („Bring Your Own Device") – zariadení, ktoré nie sú v správe a priamej kontrole IKT verejného obstarávateľa. Implementované riešenie zjednotí, zjednoduší a urýchli správu prístupov v rámci siete verejného obstarávateľa a to prostredníctvom implementácie štandardu IEEE 802.1X pre autentifikáciu a autorizáciu zariadení, ktoré budú nadväzovať spojenie so sieťou verejného obstarávateľa. Správa prístupových práv a politík sa požaduje realizovať na úrovni portov aktívnych sieťových prvkov. Súčasťou predmetu plnenia je dodávka aktívnych sieťových prvkov vrátane realizácie inštalačných a konfiguračných služieb, ktoré zabezpečia vytvorenie a možnosť prevádzky bezpečnostného protokolu IEEE 802.1X v prostredí siete verejného obstarávateľa.

Pre účely vybudovania systému overovania prostredníctvom IEEE 802.1X požaduje verejný obstarávateľ dodávku riešenia s nasledovnými minimálnymi parametrami:

Platforma pre správu prístupov	
Požadované vlastnosti	**Hodnota**
Centralizovaný manažment a správa	• centrálna konfigurácia a správa profilov, prístupov, hostí, autentifikácia a autorizácia služieb v jednoduchom web grafickom rozhraní;
Riadenie politík	• možnosť nastavovania politík prístupu na základe definovaných pravidiel; • možnosť tvorby modelov prístupu na základe definície rôznych atribútov ako sú identita používateľa / zariadenia, autentifikačné protokoly, identita koncového zariadenia; • možnosť dynamickej definície a nastavovania atribútov; • možnosť integrácie na Microsoft Active Directory, LDAP, RADIUS, RSA OTP.
Riadenie prístupov	• na základe Access Control Lists (dACLs), priradeniu k VLAN, URL presmerovania, ACLs, SGACLs.
Riadenie šifrovania	• možnosť editácie zoznamu používaného šifrovania, ktoré môže byť zakázané pre účely vynútenia bezpečnostných politík organizácie; • možnosť vynútenia využívania povoleného typu šifrovania pri autentifikácii.

AI/ML profilovanie a viacfaktorová klasifikácia	• možnosť rýchlej identifikácie neznámych koncových zariadení prostredníctvom cloudového ML engine; • možnosť revízie zariadení prostredníctvom profilových politík použitím ML engine; • možnosť tvorby prístupových skupín koncových zariadení prostredníctvom profilov a pravidiel vytvorených správcom siete;
Prístup do siete	• možnosť rýchleho nasadenia zabezpečeného prístupu k sieti prostredníctvom autentifikácie a autorizácie na základe údajov získaných z prihlasovacích údajov na rôznych aplikačných úrovniach.
Riadenie politiky prístupových skupín	• podpora jednoduchej segmentácie prostredníctvom bezpečnostných tagov; • funkcionalita správy segmentácie a zjednodušenej správy prepínačov, smerovačov, bezdrôtových zariadení a pravidiel pre firewally.
Pridávanie zariadení do siete	• podpora automatizovaného poskytovania a registrácie certifikátu pre štandardné PC a mobilné zariadenia;
AAA služby	• podpora RADIUS protokolu pre autentifikáciu, autorizáciu a accouting (AAA); • podpora protokolov PAP, MS-CHAP, EAP-MD5, PEAP, EAP-Flexible, TEAP; • podpora autentifikácie cez tunel prostredníctvom protokolu FAST, TLS, TTLS.
Správa prístupov zariadení	• podpora protokolu TACACS+; • podpora prístupu používateľa na základe lokality, skupiny, prihlasovacích údajov;
Profilovanie zariadení	• podpora preddefinovaných šablón koncových zariadení ako sú IP telefóny, kamery, smartfóny, tablety, tlačiarne; • možnosť tvorby vlastných šablón zariadení pre potreby automatického zistenia, klasifikácie a priradenia identít pri pripájaní sa do siete; • možnosť priraďovania autorizačných politík špecifických pre koncový bod na základe identifikovaného typu zariadenia; • možnosť zberu údajov o atribútoch koncového bodu pomocou pasívneho monitorovania siete a telemetrie.
Hodnotenie zariadení pripojených do siete	• podpora vyhodnocovania koncových zariadení pripojených v sieti; • podpora vytvárania politík na kontrolu najnovších záplat OS, kontrolu aktuálnych verzií antivírusových a antispyware balíkov, kontrolu pravidiel šifrovania disku, prítomnosti aplikácií a pod. • podpora plnej viditeľnosti HW zariadení v sieti;
Podpora Active Directory	• podpora autentifikácie a autorizácie použitím multistromových Microsoft AD domén; • podpora grupovania viacerých nespojených domén do logických skupín; • možnosť flexibilného prepisovania pravidiel identít;

	• podpora Microsoft AD 2003, 2008, 2008R2, 2012, 2012R2, 2016 a 2019
Monitoring a riešenie problémov	• integrovaná konzola s webovým rozhraním pre účely monitorovania, generovania správ a riešenia problémov; • podporuje funkcionalitu záznamu všetkých aktivít a metrík v reálnom čase na úrovni všetkých používateľov a koncových bodov, ktoré sú pripojené v sieti.
Spôsob nasadenia	• možnosť nasadenia v prostredí verejného obstarávateľa v režime vysokej dostupnosti „HA". Prostredie virtualizácie a výpočtové zdroje poskytne verejný obstarávateľ.
Licencia	• rozsah licencie pre minimálne 1500 autentifikovaných zariadení; • platnosť licencie musí byť min. 12 kalendárnych mesiacov.
Servisná podpora	• požaduje sa poskytnutie servisnej podpory min. na obdobie 12 kalendárnych mesiacov.
Ďalšie požiadavky	• súčasťou dodávky sú analytické práce, inštalácia, uvedenie do prevádzky, otestovanie a nasadenie riešenia pre správu prístupov koncových zariadení.

Verejný obstarávateľ za účelom kontroly, správy a riadenia prístupov koncových zariadení do siete na úrovni potrov na aktívnych prvkoch potrebuje obstarať, nasadiť a nakonfigurovať súčasne nové, nepoužité switche, ktoré podporujú protokol IEEE 802.1X pre autentifikáciu a autorizáciu zariadení pristupujúcich do siete. Verejný obstarávateľ požaduje obstarať nasledovné typy aktívnych prvkov s nasledovnou minimálnou technickou špecifikáciou:

Switch TYP 1 (7ks)	
Požadované vlastnosti	**Hodnota**
Porty	• 24 portov 10/100/1000 Ethernet PoE+
Uplink rozhrania	• 4 x 1G SPF uplink
CPU	• ARM v 7 800 MHz
PoE+ power budget	• 195 W
DRAM	• 512 MB
Flash pamäť	• 256 MB
Šírka pásma – forwarding	• 28 Gbps
Šírka pásma – switching	• 56 Gbps
Rýchlosť preposielania (64 byte L3 paketov)	• 41,67 Mpps
Unicast MAC adresy	• 16000
IPv4 unicast direct routes	• 542
IPv4 unicast indirect routes	• 256
IPv6 unicast direct routes	• 414
IPv6 inicast indirect routes	• 128
IPv4 multicast routes a IGMP skupiny	• 1024

IPv6 multicast skupiny	• 1024
Maximálny počet aktívnych VLAN	• 256
MTU-L3 paket	• 9198 bajtov
Jumbo ethernet rámce	• 10 240 bajtov

Súčasťou dodávky bude ich doprava na miesto, inštalácia a konfigurácia nových, nepoužitých zariadení. Súčasťou ponuky uchádzača je zabezpečenie všetkých potrebných licencií pre obstarávané zariadenia na obdobie minimálne 12 kalendárnych mesiacov.

Plnenie aktivity bude súčasne pozostávať z poskytnutia služieb – činností nasledovných expertov:

Názov pozície	**Merná jednotka (m.j.)**	**Počet m.j.**
Projektový manažér IT projektu	*Človekodeň (MD)*	*5*
IT analytik	*Človekodeň (MD)*	*2*
Špecialista pre bezpečnosť IT	*Človekodeň (MD)*	*4*
Špecialista pre infraštruktúrny/HW špecialista	*Človekodeň (MD)*	*11*
IT tester	*Človekodeň (MD)*	*2*
Školiteľ pre IT systémy	*Človekodeň (MD)*	*1*
SPOLU	**Človekodeň (MD)**	**25**

3. Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky

Verejný obstarávateľ požaduje od uchádzača vykonať realizáciu segmentácie siete v kontexte analýzy siete, ktorú bude nevyhnutné za týmto účelom vykonať. Predmetom zákazky v rámci tejto aktivity budú plánovanie segmentácie v kontexte identifikovaných možných logických segmentov s ohľadom na topológiu siete, prevádzkované agendové IS, výstupy realizovanej inventarizácie aktív a klasifikácie informácií a kategorizácie ako aj bezpečnostné požiadavky a požiadavky na výkonnosť. Predmetom dodávky bude vykonané mapovanie siete s cieľom získania komplexného a presného obrazu o existujúcej sieti verejného obstarávateľa vrátane všetkých relevantných informačných aktív.

V rámci realizovanej aktivity bude vykonané rozdelenie rozsahov IP adries v rámci vytváraných segmentov, pričom pre každé aktívum budú pridelené IP adresy z definovaných rozsahov. V rámci plnenia budú v kontexte novo dodávaných sieťových prvkov prehodnotené fyzické segmenty siete a z nich vychádzajúce logické segmenty pomocou VLAN. Dodávateľ v rámci dodávky vykoná konfiguráciu dotknutých zariadení (switche, routre, firewally) tak, aby nastavenia zodpovedali schválenému návrhu segmentácie verejným obstarávateľom. Súčasťou predmetu plnenia bude vypracovanie komplexnej dokumentácie zachytávajúce celý stav vykonanej segmentácie, vrátane otestovania a overenia funkcionality.

Pre upresnenie verejný obstarávateľ uvádza, že požaduje vykonať horeuvedené činnosti v rozsahu veľkosti siete v ktorej je aktívne využívaných 85 switchov, 40 routerov, 2 firewally vrátane zariadení, ktoré sú predmetom dodávky v rámci tohto projektu.

Plnenie bude pozostávať z poskytnutia služieb – činností nasledovných expertov:

Názov pozície	Merná jednotka (m.j.)	Počet m.j.
Projektový manažér IT projektu	*Človekodeň (MD)*	*9*
IT analytik	*Človekodeň (MD)*	*15*
Špecialista pre infraštruktúrny/HW špecialista	*Človekodeň (MD)*	*16*
Špecialista pre bezpečnosť IT	*Človekodeň (MD)*	*7*
IT tester	*Človekodeň (MD)*	*2*
SPOLU	**Človekodeň (MD)**	**49**

4. Dodávka aktívnych prvkov CORE časti siete

Verejný obstarávateľ v rámci plánovaných aktivít požaduje dodať nové, nepoužité, v originálnom obale zabalené aktívne prvky CORE časti siete zodpovedajúce minimálnym požiadavkám identifikovaným nižšie v tomto dokumente. Výmena sa požaduje s ohľadom na potrebu nahradenia end-of-sales and end-of-support aktívnych prvkov ako aj doplnenie jestvujúcich ako aj s ohľadom na potrebu zabezpečenia väčšej bezpečnosti prevádzky siete ako aj prenosovej kapacity siete ako reakciou na neustále rastúce požiadavky na prenos v sieti verejného obstarávateľa. Výmenou potrebných aktívnych prvkov CORE časti siete verejný obstarávateľ očakáva zároveň zabezpečiť kontinuitu požadovanej úrovne IT aktív ako aj primerané doby odozvy informačných aktív prevádzkovaných verejným obstarávateľom. Výmena aktívnych prvkov CORE časti siete je potrebná aj s ohľadom na zámere verejného obstarávateľa implementovať systém pre riadenie správy a prístupov koncových zariadení do siete verejného obstarávateľa a implementovať protokol IEEE 802.1X. Súčasný stav CORE časti siete neumožňuje plnohodnotné nasadenie IEEE 802.1X v rozsahu očakávanej segmentácie siete zahŕňajúcej okrem nových CORE aktívnych prvkov aj obstarané aktívne prvky v rámci aktivity 3. tejto Výzvy. Verejný obstarávateľ požaduje obstarať celkovo 9 ks aktívnych prvkov CORE časti siete. Súčasťou dodávky nových, nepoužitých zariadení zabalených v originálnom balení, bude ich inštalácia, konfigurácia a uvedenie do prevádzky tak, aby mohli dodávané zariadenia byť zahrnuté do výkonu segmentácie siete verejného obstarávateľa ako aj nasadenia overovania podľa IEEE 802.1X.

Súčasťou dodávky bude implementácia riešenia zberu prevádzkových údajov zo zariadení Firewall CORE časť – TYP 1 s nasledovnou minimálnou funkcionalitou:

- Korelácia udalostí a detekcia v reálnom čase na úrovni všetkých zberaných logov;
- Detekcia pokročilých hrozieb;
- Real-time prehľady a historické náhľady o aktivite na sieti verejného obstarávateľa;
- Prehľad o spustených aplikáciách, zdrojoch, cieľoch, webových stránkach, bezpečnostných hrozbách a systémových udalostiach.

Verejný obstarávateľ požaduje obstarať nasledovné typy aktívnych prvkov CORE časti siete s nasledovnou minimálnou technickou špecifikáciou:

Firewall CORE časť - TYP 1 (2 ks)	
Požadované vlastnosti	**Hodnota**

GE RJ-45 porty	• 16 ks
GE RJ-45 porty – manažment HA	• 1 ks
GE SFP slot	• 8 ks
10 GE SFP+	• 2 ks
USB port	• 1 ks
Konzolový port	• 1 ks
Vnútorné úložisko	• 480 GB SSD
IPS priepustnosť	• 5 Gbps
NGFW priepustnosť	• 3.5 Gbps
Ochrana pred hrozbami – priepustnosť	• 3 Gbps
UPv4 priepustnosť firewallu (1518 / 512 / 64 bajtov, UDP)	• 27 / 27 / 11 Gbps
Priepustnosť firewallu (paket / sekunda)	• 16.5 Mpps
Počet súčasných spojení (TCP)	• 3 000 000
Počet nových spojení TCP / sekunda	• 280 000
Počet politík FW	• 10 000
Priepustnosť IPsec VPN (256 bajtov)	• 13 Gbps
Počet GW to GW IPsec VPN tunelov	• 2 000
Počet klient–klient IPsec VPN tunelov	• 16 000
Priepustnosť SSL-VPN	• 2 Gbps
Počet súčasných SSL-VPN používateľov	• 500
Priepustnosť SSL inšpekcie	• 4 000 Gbps
SSL inšpekcia CPS	• 3 500
Počet súčasných spojení SSL inšpekcia	• 300 000
Priepustnosť kontroly aplikácií	• 13 Gbps
CAPWAP priepustnosť	• 20 Gbps
Počet virtuálnych domén	• 10
HA konfigurácia	• active-active, active-passive, clustering

Switch CORE časť - TYP 1 (2 ks)	
Požadované vlastnosti	**Hodnota**
10/100/1000 porty	• 24x 1G SFP
Pamäť DRAM	• 8 GB
Pamäť flash	• 16 GB
Počet VLAN IDs	• 4094
Uplink konfigurácia	• Modulárna
Kapacita prepínania	• 208 Gbps

Prepínacia kapacita vrátane stackovania	• 688 Gbps
Rýchlosť preposielania	• 154,76 Mpps
Celový počet MAC adries	• 32 000
IPv4 direct routes	• 24 000
IPv4 indirect routes	• 8 000
IPv6 routes	• 16 000
Rozsah multicast routing	• 8 000
Rozsah QoS záznamov	• 5 120
Rozsah ACL záznamov	• 5 120
Jumbo ethernet rámce	• 9198 bajtov
Príslušenstvo – stohovací kábel 1	• 2x stohovací kábel; • Kompatibilný so Switch CORE TYP 1; • Dĺžka 0,5 m.
Príslušenstvo – stohovací kábel 2	• 2ks stohovací kábel; • Kompatibilný so Switch CORE TYP 1; • Možnosť sériového napájania zariadení; • Dĺžka 1,5 m.
Príslušenstvo – sieťový modul	• 10 GE SFP+; • Rýchlosť 1G/10Gb/s; • Chladenie pasívne; • Kompatibilita so Switch CORE TYP1.
Príslušenstvo – napájací zdroj	• redundantný napájací zdroj – dva zdroje; • Kompatibilný so Switch CORE TYP 1; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 715 W.
Príslušenstvo – SFP+ modul	• 12 ks SPF+ modul; • Kompatibilita so Switch CORE TYP1.

Switch CORE časť - TYP 2 (2 ks)	
Požadované vlastnosti	**Hodnota**
10/100/1000 porty	• 24x 1G metalické
Pamäť DRAM	• 8 GB
Pamäť flash	• 16 GB
Počet VLAN IDs	• 4094
Uplink konfigurácia	• Modulárna
Kapacita prepínania	• 208 Gbps
Prepínacia kapacita vrátane stackovania	• 688 Gbps
Rýchlosť preposielania	• 154,76 Mpps
Celový počet MAC adries	• 32 000
IPv4 direct routes	• 24 000
IPv4 indirect routes	• 8 000
IPv6 routes	• 16 000
Rozsah multicast routing	• 8 000
Rozsah QoS záznamov	• 5 120
Rozsah ACL záznamov	• 5 120
Jumbo ethernet rámce	• 9198 bajtov

Príslušenstvo – stohovací kábel 2	• 2ks stohovací kábel; • Kompatibilný so Switch CORE TYP 2; • Možnosť sériového napájania zariadení; • Dĺžka 1,5 m.
Príslušenstvo – sieťový modul	• 10 GE SFP+; • Rýchlosť 1G/10Gb/s; • Chladenie pasívne; • Kompatibilita so Switch CORE TYP2.
Príslušenstvo – napájací zdroj	• Redundantný napájací zdroj - dva zdroje; • Kompatibilný so Switch CORE TYP 2; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 350 W.

Switch CORE časť - TYP 3 (1 ks)	
Požadované vlastnosti	**Hodnota**
10/100/1000 porty	• 24
Pamäť DRAM	• 2 GB
Pamäť flash	• 4 GB
Počet VLAN IDs	• 4096
Kapacita prepínania	• 128 Gbps
Stakovacia šírka pásma	• 80 Gbps
Rýchlosť preposielania	• 95,23 Mpps
Celkový počet MAC adries	• 16 000
IPv4 direct routes	• 8 000
IPv4 indirect routes	• 3 000
IPv6 routes	• 1 500
Rozsah multicast routing	• 1 000
Rozsah QoS záznamov	• 1 000
Rozsah ACL záznamov	• 1 500
Jumbo ethernet rámce	• 9 198 bajtov
Príslušenstvo – napájací zdroj	• redundantný napájací zdroj – dva zdroje; • Kompatibilný so Switch CORE TYP 3; • Možnosť napájania z elektrickej siete; • Výkon zdroja min. 125 W.

Router CORE časť - TYP 1 (2 ks)	
Požadované vlastnosti	**Hodnota**
10/100/1000 porty	• 24x 1G SFP
Pamäť DRAM	• 4 GB
Pamäť flash	• 2 GB
Ethernet LAN	• Áno
Podpora L2 VPN	• Áno
Podpora L3 VPN	• Áno
Rýchlosť prenosu	• 1 000, 10 000 Mbit/s
Podpora QoS	• Áno
Príslušenstvo – SFP+ modul	• 2 ks SPF+ modul; • Kompatibilita so Router časť CORE TYP1.

Súčasťou dodávky nových, nepoužitých a originálne od výrobcu zabalených tovarov bude ich doprava na miesto, inštalácia a konfigurácia, vrátane inštalácie potrebnej kabeláže. Súčasťou ponuky uchádzača je zabezpečenie všetkých potrebných licencií pre obstarávané zariadenia na obdobie minimálne 12 kalendárnych mesiacov.

Plnenie aktivity bude súčasne pozostávať z poskytnutia služieb – činností nasledovných expertov:

Názov pozície	**Merná jednotka (m.j.)**	**Počet m.j.**
Projektový manažér IT projektu	*Človekodeň (MD)*	*5*
IT analytik	*Človekodeň (MD)*	*2*
Špecialista pre bezpečnosť IT	*Človekodeň (MD)*	*4*
Špecialista pre infraštruktúrny/HW špecialista	*Človekodeň (MD)*	*11*
IT tester	*Človekodeň (MD)*	*2*
Školiteľ pre IT systémy	*Človekodeň (MD)*	*1*
SPOLU	**Človekodeň (MD)**	**25**

5. Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

Verejný obstarávateľ v rámci navrhovaného riešenia požaduje implementovať riešenie pre vzdialený prístup vrátane mobilných tokenov a autentifikačného servera vyžadujúceho druhý stupeň overenia užívateľa prihlasujúceho sa do internej siete prostredníctvom implementácie služby 2-faktorového overovania („2FA") pre celkovo 700 používateľov pristupujúcich do siete verejného obstarávateľa.

Požaduje sa, aby implementovaný autentifikačný server od užívateľa vyžadoval zadanie mena a hesla a následne po úspešnom zadaní prihlasovacej kombinácie vyžiadal zadanie jednorazového hesla, ktoré bude možné užívateľom generovať prostredníctvom dodaného hardvérového a softvérového tokenu kompatibilného s mobilnými zariadeniami iOS, Android a Windows, čím sa zabezpečí ďalšia úroveň zabezpečenia prístupu do siete Verejného obstarávateľa z vonkajšieho prostredia.

Súčasťou poskytovanej služby je dodanie VPN klientov s bezpečnostným modelom s nulovou dôverou, teda VPN klient, ktorý zároveň disponuje funkcionalitou kontroly koncového zariadenia voči nastaveným prístupovým politikám. VPN klient bude zároveň disponovať funkcionalitou karantény pripájajúcich sa koncových zariadení a umožní izolovať napadnuté koncové zariadenia od zvyšku siete, čím sa minimalizuje ohrozenie internej siete z podozrivého zdroja.

Požiadavky na predmet zákazky:

Autentifikátor

- Počet užívateľov: 700;

- Počet mobilných SW tokenov: 650;
- Počet HW tokenov: 50;
- Počet užívateľských certifikátov: 700;
- Nasadenie vo VM úspešného poskytovateľa;
- Podpora hypervízorov: VMware ESXi/ ESX 6ú7/8, Microsoft Hyper-V Server 2010, 2012 RC a 2016, KVM, Xen, Microsoft Azure, AWS, Nutanix AHV, Oracle OCI, Alibaba Cloud;
- Podpora režimu vysokej dosutpnosti („HA");
- Možnosť upgrade licencie min. na dvojnásobok voči požadovanej kapacite;

Mobilný SW token / HW token

- V prípade SW tokenu, mobilná aplikácia kompatibilná s mobilnými zariadeniami iOS, Android, Windows;
- V prípade HW tokenu – prenosné zariadenie napr. vo forme kľúčenky.
- Požadovaný počet licencií pre koncové zariadenia: 700;
- inštalácia na mobilné zariadenia Verejného obstarávateľa (v prípade SW tokenu);
- funkcionalita generovania jednorazového hesla;
- dynamické generovanie hesiel;
- kompatibilita s ponúknutým VPN klientom a jestvujúcou infraštruktúrou Verejného obstarávateľa;
- overovanie užívateľov musí služba zabezpečovať prostredníctvom samostatného autentifikačného servera;
- podpora time-based ako aj event-based tokenov;
- kompatibilita s OATH.

VPN KLIENT

- Počet užívateľov: 700;
- Inštalácia na zariadenia Verejného obstarávateľa;
- Možnosť konfigurácie zero trust pravidiel prístupu do siete;
- Možnosť centrálneho manažmentu;
- Centralizované logovanie a reporting;
- Podpora IPSEC VPN a SSL VPN s viacfatorovým overením (podpora mobilného SW tokenu – kompatibilita s navrhovaným riešením Uchádzača);
- Podpora webfilteringu;
- Podpora výrobcu 24/7;
- On premise inštalácia;
- Jednoduché a prehľadné užívateľské prostredie;
- Podpora integrácie na Active Directory;
- Dynamické riadenie prístupu;
- Podpora užívateľských skupín;
- Podpora dynamickej voľby brány.

Manažment koncových zariadení

- Funkcionalita manažmentu koncových zariadení;
- Požaduje sa nasadenie v infraštruktúre dodávateľa;
- Podpora vzdialenej správy VPN klientov;

- Možnosť priraďovania bezpečnostných profilov pre skupiny koncových zariadení;
- podpora nasadzovania VPN klientov;
- správa aktualizácií a verzií VPN klientov;
- užívateľský dashboard;
- možnosť integrácie na Active Directory;
- automatické generovanie definovaných alertov;
- centralizovaný provisioning užívateľov;
- možnosť centralizovaného update VPN klientov;
- možnosť centralizovanej správy užívateľských skupín;
- funkcionalita karantény koncových zariadení;
- automatizovaný monitoring koncových zariadení (verzie, OS IP/MAC adresy, stav koncových zariadení).

Plnenie bude okrem nákupu HW/SW komponentov pozostávať z poskytnutia služieb – činností expertov v oblasti IB a KB v nasledovnom rozsahu:

Názov pozície	**Merná jednotka (m.j.)**	**Počet m.j.**
Projektový manažér IT projektu	*Človekodeň (MD)*	*4*
IT analytik	*Človekodeň (MD)*	*2*
Špecialista pre bezpečnosť IT	*Človekodeň (MD)*	*4*
IT tester	*Človekodeň (MD)*	*1*
Špecialista pre infraštruktúrny/HW špecialista	*Človekodeň (MD)*	*3*
Školiteľ pre IT systémy	*Človekodeň (MD)*	*1*
SPOLU	**Človekodeň (MD)**	**15**

6. Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

Verejný obstarávateľ požaduje implementovať ucelené riešenie prevencie a detekcie pred hrozbami z vonkajšieho prostredia. Riešenie bude zabezpečovať centrálnu správu ochrany koncových staníc, detekciu nevyžiadanej aktivity na koncových staniciach, anti-malware ochranu, funkcionalitu firewallu na úrovni koncového zariadenia, funkcionalitu monitoringu prevádzky na koncových zariadeniach, funkcionalitu web-filteringu, karantény, antivíru, skenovania koncových zariadení ako aj funkcionalitu automatickej karantény a možnosti centrálneho nastavovania bezpečnostných pravidiel a politík pre koncové zariadenia.

Verejný obstarávateľ požaduje obstarať ucelený centralizovaný systém správy ochrany koncových staníc o celkovom počte 700 ks s nasledovnou minimálnou technickou špecifikáciou:

Platforma pre centralizovanú ochranu a správu 700 ks koncových staníc	
Požadované vlastnosti	**Hodnota**
Centrálna správa a manažment koncových zariadení	• jednoduché používateľské grafické rozhranie centralizovaného manažmentu; • možnosť diaľkového nasadenia klientov na koncové zariadenia;

	• údaje o prevádzke na koncovej stanici zobrazované v reálnom čase; • integrácia na Active Directory; • centrálna správa karantény; • možnosť priraďovania koncových zariadení do skupín; • automatizované notifikácie; • centralizovaný provisioning klientov; • automatické reakcie systému na hrozby; • možnosť centralizovaného SW na koncovej stanici; • ochrana SSL VPN klienta;
Telemetria a monitoring koncových zariadení	• informácie a klientovi na koncovej stanici (verzia, OS, IP/MAX adresa, profil užívateľa); • stav klientskej stanice; • možnosť reportovania telemetrie na úrovni centrálnej správy;
Kompatibilita riešenia pre koncové stanice	• MS Windows, MacOS, iOS, Linux.

Súčasťou dodania bude analýza prostredia verejného obstarávateľa, konfigurácia krabicového SW riešenia pre potreby organizácie, jeho inštalácia/implementácia v prostredí verejného obstarávateľa, ktorá bude zabezpečená prostredníctvom činností rolí expertov pre oblasť IB a KB.

Názov pozície	**Merná jednotka (m.j.)**	**Počet m.j.**
Projektový manažér IT projektu	*Človekodeň (MD)*	*4*
IT analytik	*Človekodeň (MD)*	*2*
Špecialista pre bezpečnosť IT	*Človekodeň (MD)*	*4*
IT tester	*Človekodeň (MD)*	*2*
Špecialista pre infraštruktúrny/HW špecialista	*Človekodeň (MD)*	*3*
SPOLU	**Človekodeň (MD)**	**15**

Uchádzač do ponúkanej ceny zahrnie servisnú podporu od výrobcu vrátane aktualizácii SW na obdobie 60 mesiacov v režime 8 x 5 x next business day, a postimplementačnú podporu (technickú podporu a servis prevádzkovaných informačných technológií počas záručnej doby).

Príloha č.2 Zmluvy

Zoznam odborných kapacít Zhotoviteľa

Príloha č.2 k Zmluve o dielo č. ...../2025/OIT „Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica“ – Zoznam odborných kapacít

Poradie	Pozícia	Meno a priezvisko	Poznámka
1	Projektový manažér IT projektu	Michal Jandura	
2	Expert pre oblasť riadenia služieb IB/KB	Lukáš Karlík	
3	HW špecialista	Miroslav Habánik	
4	Špecialista pre bezpečnosť IT	Peter Ondrejkovič	
5	Špecialista pre bezpečnosť IT (procesný garant)	Jozef Priesol	

Príloha č.3 Zmluvy

Zoznam subdodávateľov

Príloha č. 3 k Zmluve o dielo č. ...../2025/OIT „Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica“

Zoznam subdodávateľov

Meno a podrobnosti o subdodávateľovi (názov, sídlo, IČO)	Práce/služby určené pre subdodávateľa	Osoba oprávnená konať za subdodávateľa (meno a priezvisko, adresa pobytu, dátum narodenia)	% podiel subdodávky na celkovej Cene za Dielo
			0,00%
			0,00%
			0,00%
			0,00%
			0,00%
			0,00%

V Bratislave, dňa

.....

RNDr. Lukáš Karlík, PhD.

Príloha č.4 Zmluvy

Rozpočet (Súťažná cenová ponuka Zhotoviteľa)

Príloha č.4 k Zmluve o dielo č. ...../2025/OIT „Zvýšenie úrovne kybernetickej a informačnej bezpečnosti Mesta Banská Bystrica"

Rozpočet položkový

„Zvýšenie úrovne informačnej a kybernetickej bezpečnosti v Meste Banská Bystrica"

Aktivita 1 : Vypracovanie relevantnej bezpečnostnej dokumentácie

Etapa	Názov položky	Merná jednotka	Počet m.j.	Jednotk. Cena v € bez DPH	Cena celkom v € bez DPH	DPH 23%	Cena celkom v € s DPH
Analýza dizajn	Projektový manažér IT projektu	MD	5	500,00 €	2 500,00 €	575,00 €	3 075,00 €
Analýza dizajn	IT analytik	MD	35	500,00 €	17 500,00 €	4 025,00 €	21 525,00 €
Implementácia a testovanie	Špecialista pre bezpečnosť IT	MD	10	600,00 €	6 000,00 €	1 380,00 €	7 380,00 €
Implementácia a testovanie	Špecialista pre infraštruktúrny/HW špecialista	MD	5	550,00 €	2 750,00 €	632,50 €	3 382,50 €
Nasadenie	Špecialista pre databázy	MD	5	550,00 €	2 750,00 €	632,50 €	3 382,50 €
Nasadenie	IT/IS konzultant	MD	25	550,00 €	13 750,00 €	3 162,50 €	16 912,50 €
Spolu					**45 250,00 €**	**10 407,50 €**	**55 657,50 €**

Aktivita 2: Implementácia a konfigurácia systému pre riadenie správy prístupov koncových zariadení do siete Mesta

Etapa	Názov položky	Merná jednotka	Počet m.j.	Jednotk. Cena v € bez DPH	Cena celkom v € bez DPH	DPH 23%	Cena celkom v € s DPH
Nákup HW, SW a služieb	Platforma pre správu prístupov	ks	1	28 900,00 €	28 900,00 €	6 647,00 €	35 547,00 €
Nákup HW, SW a služieb	Switch Typ 1	ks	7	890,00 €	6 230,00 €	1 432,90 €	7 662,90 €
Analýza dizajn	IT analytik	MD	2	500,00 €	1 000,00 €	230,00 €	1 230,00 €
Analýza dizajn	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Implementácia a testovanie	Špecialista pre infraštruktúrny/HW špecialista	MD	10	550,00 €	5 500,00 €	1 265,00 €	6 765,00 €
Implementácia a testovanie	Špecialista pre bezpečnosť IT	MD	4	600,00 €	2 400,00 €	552,00 €	2 952,00 €
Implementácia a testovanie	Projektový manažér IT projektu	MD	3	500,00 €	1 500,00 €	345,00 €	1 845,00 €
Implementácia a testovanie	IT tester	MD	2	450,00 €	900,00 €	207,00 €	1 107,00 €
Nasadenie	Špecialista pre infraštruktúrny/HW špecialista	MD	1	550,00 €	550,00 €	126,50 €	676,50 €
Nasadenie	Školiteľ pre IT systémy	MD	1	450,00 €	450,00 €	103,50 €	553,50 €
Nasadenie	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Spolu					**48 430,00 €**	**11 138,90 €**	**59 568,90 €**

Aktivita 3: Vykonanie segmentácie siete s ohľadom na súčasné prevádzkové požiadavky;

Etapa	Názov položky	Merná jednotka	Počet m.j.	Jednotk. Cena v € bez DPH	Cena celkom v € bez DPH	DPH 23%	Cena celkom v € s DPH
Analýza dizajn	IT analytik	MD	15	500,00 €	7 500,00 €	1 725,00 €	9 225,00 €
Analýza dizajn	Špecialista pre IT bezpečnosť	MD	2	600,00 €	1 200,00 €	276,00 €	1 476,00 €
Analýza dizajn	Projektový manažér IT projektu	MD	3	500,00 €	1 500,00 €	345,00 €	1 845,00 €
Implementácia a testovanie	Špecialista pre infraštruktúrny/HW špecialista	MD	14	550,00 €	7 700,00 €	1 771,00 €	9 471,00 €
Implementácia a testovanie	Špecialista pre bezpečnosť IT	MD	5	600,00 €	3 000,00 €	690,00 €	3 690,00 €
Implementácia a testovanie	IT tester	MD	2	450,00 €	900,00 €	207,00 €	1 107,00 €
Implementácia a testovanie	Projektový manažér IT projektu	MD	5	500,00 €	2 500,00 €	575,00 €	3 075,00 €
Nasadenie	Špecialista pre infraštruktúrny/HW špecialista	MD	2	550,00 €	1 100,00 €	253,00 €	1 353,00 €
Nasadenie	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
					25 900,00 €	**5 957,00 €**	**31 857,00 €**

Aktivita 4: **Dodávka aktívnych prvkov CORE časti siete**

Etapa	Názov položky	Merná jednotka	Počet m.j.	Jednotk. Cena v € bez DPH	Cena celkom v € bez DPH	DPH 23%	Cena celkom v € s DPH
Nákup HW, SW a služieb	Firewall CORE časť - TYP 1	ks	2	21 900,00 €	43 800,00 €	10 074,00 €	53 874,00 €
Nákup HW, SW a služieb	Switch CORE časť - TYP 1	ks	2	16 900,00 €	33 800,00 €	7 774,00 €	41 574,00 €
Nákup HW, SW a služieb	Switch CORE časť - TYP 2	ks	2	4 790,00 €	9 580,00 €	2 203,40 €	11 783,40 €
Nákup HW, SW a služieb	Switch CORE časť - TYP 3	ks	1	4 900,00 €	4 900,00 €	1 127,00 €	6 027,00 €
Nákup HW, SW a služieb	Router CORE časť - TYP 1	ks	2	2 690,00 €	5 380,00 €	1 237,40 €	6 617,40 €
Analýza dizajn	IT analytik	MD	2	500,00 €	1 000,00 €	230,00 €	1 230,00 €
Analýza dizajn	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Implementácia a testovanie	Špecialista pre infraštruktúrny/HW špecialista	MD	10	550,00 €	5 500,00 €	1 265,00 €	6 765,00 €
Implementácia a testovanie	Špecialista pre bezpečnosť IT	MD	4	600,00 €	2 400,00 €	552,00 €	2 952,00 €
Implementácia a testovanie	Projektový manažér IT projektu	MD	3	500,00 €	1 500,00 €	345,00 €	1 845,00 €
Implementácia a testovanie	IT tester	MD	2	450,00 €	900,00 €	207,00 €	1 107,00 €
Nasadenie	Špecialista pre infraštruktúrny/HW špecialista	MD	1	550,00 €	550,00 €	126,50 €	676,50 €
Nasadenie	Školiteľ pre IT systémy	MD	1	450,00 €	450,00 €	103,50 €	553,50 €
Nasadenie	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Spolu					**110 760,00 €**	**25 474,80 €**	**136 234,80 €**

Aktivita 5: Implementácia systému dvojfaktorovej autentifikácie pre vzdialený prístup do vnútornej siete

Etapa	Názov položky	Merná jednotka	Počet m.j.	Jednotk. Cena v € bez DPH	Cena celkom v € bez DPH	DPH 23%	Cena celkom v € s DPH
Nákup HW, SW a služieb	SW riešenie dvojfaktorovej autentifikácie	ks	1	13 900,00 €	13 900,00 €	3 197,00 €	17 097,00 €
Nákup HW, SW a služieb	Mobilný SW token pre 650 užívateľov	ks	1	11 490,00 €	11 490,00 €	2 642,70 €	14 132,70 €
Nákup HW, SW a služieb	HW token	ks	50	40,00 €	2 000,00 €	460,00 €	2 460,00 €
Analýza dizajn	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Analýza dizajn	IT analytik	MD	2	500,00 €	1 000,00 €	230,00 €	1 230,00 €
Analýza dizajn	Špecialista pre bezpečnosť IT	MD	2	600,00 €	1 200,00 €	276,00 €	1 476,00 €
Analýza dizajn	Špecialista pre infraštruktúrny/HW špecialista	MD	1	550,00 €	550,00 €	126,50 €	676,50 €
Implementácia a Testovanie	Projektový manažér IT projektu	MD	2	500,00 €	1 000,00 €	230,00 €	1 230,00 €
Implementácia a Testovanie	Špecialista pre bezpečnosť IT	MD	2	600,00 €	1 200,00 €	276,00 €	1 476,00 €
Implementácia a Testovanie	IT tester	MD	1	450,00 €	450,00 €	103,50 €	553,50 €
Implementácia a Testovanie	Špecialista pre infraštruktúrny/HW špecialista	MD	1	550,00 €	550,00 €	126,50 €	676,50 €
Nasadenie	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Nasadenie	Špecialista pre infraštruktúrny/HW špecialista	MD	1	550,00 €	550,00 €	126,50 €	676,50 €
Nasadenie	Školiteľ pre IT systémy	MD	1	450,00 €	450,00 €	103,50 €	553,50 €
	Spolu				35 340,00 €	8 128,20 €	43 468,20 €

Aktivita 6: Implementácia riešenia centrálneho bezpečnostného manažmentu pre koncové stanice

Etapa	Názov položky	Merná jednotka	Počet m.j.	Jednotk. Cena v € bez DPH	Cena celkom v € bez DPH	DPH 23%	Cena celkom v € s DPH
Nákup HW, SW a služieb	Platforma pre centralizovanú ochranu a správu 700 ks koncových stanic	ks	1	23 490,00 €	23 490,00 €	5 402,70 €	28 892,70 €
Analýza dizajn	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Analýza dizajn	IT analytik	MD	2	500,00 €	1 000,00 €	230,00 €	1 230,00 €
Analýza dizajn	Špecialista pre bezpečnosť IT	MD	2	600,00 €	1 200,00 €	276,00 €	1 476,00 €
Implementácia a testovanie	Projektový manažér IT projektu	MD	2	500,00 €	1 000,00 €	230,00 €	1 230,00 €
Implementácia a testovanie	Špecialista pre bezpečnosť IT	MD	2	600,00 €	1 200,00 €	276,00 €	1 476,00 €
Implementácia a testovanie	IT tester	MD	2	450,00 €	900,00 €	207,00 €	1 107,00 €
Implementácia a testovanie	Špecialista pre infraštruktúry/HW špecialista	MD	2	550,00 €	1 100,00 €	253,00 €	1 353,00 €
Nasadenie	Projektový manažér IT projektu	MD	1	500,00 €	500,00 €	115,00 €	615,00 €
Nasadenie	Špecialista pre infraštruktúry/HW špecialista	MD	1	550,00 €	550,00 €	126,50 €	676,50 €
Spolu					**31 440,00 €**	**7 231,20 €**	**38 671,20 €**

Cena celkom: Aktivita 1 až 6 bez DPH	**297 120,00 €**
DPH 23%	**68 337,60 €**
Cena celkom: Aktivita 1 až 6 s DPH	**365 457,60 €**

V Bratislave, [illegible]

.....

RNDr. Lukáš Karlík, PhD.
(na základe plnej moci)